CONTRIBUTIONS TO THE THEORY OF LOOPS

BY
R. H. BRUCK

Introduction. It is not altogether easy to single out the dominant idea of the present paper; perhaps this may be said to be the notion of a *π-series,* which is introduced in Chapter I and recurs in Chapters II and III. Associated with this notion are the concepts of *π-nilpotent* and of *π-solvable* loops.

It would require too much space for precise definitions of these concepts here. We may say, however, that π designates some "characteristic" property which singles out certain elements of a given loop G; and that, by special choices of π, we arrive at the notions of a *centrally nilpotent* loop (analogous to a nilpotent group), of a *left-associatrally nilpotent* loop (in which the role of the centre in central nilpotency is now usurped by what we have called the normal left associator), of a *middle-associatrally nilpotent* loop, and so on. When attention is restricted to loops with the inverse property, as is the case in Chapter II, we have in addition the notions of *Moufang nilpotency* and *Moufang-central nilpotency.*

Certainly the most useful tool introduced in this paper is the *inner mapping group* $\mathfrak{J}$ of a loop G. When G is a group, $\mathfrak{J}$ reduces to the group of inner automorphisms of G. In any case, $\mathfrak{J}$ has the property of deciding normality; a subloop H of the loop G is normal in G if and only if H is mapped into itself by every element of $\mathfrak{J}$. But it is not true that $\mathfrak{J}$ always consists of automorphisms. In view of this latter fact it is necessary to learn a new technique for the purpose of calculating with $\mathfrak{J}$. A considerable part of Chapter I is in fact devoted to the theory of the inner mapping group, particularly in connection with finite centrally nilpotent loops.

Another important tool is the *autotopism group* of a loop G. We say that an ordered triple (U, V, W) of one-to-one mappings U, V, W of G upon itself is an autotopism of G if and only if $xU \cdot yV = (xy)W$ for all x, y of G. (The autotopisms form a group under the multiplication $(U, V, W)\ (U_1, V_1, W_1) = (UU_1, VV_1, WW_1)$.) As is shown in Chapter II, many interesting new structure theorems for loops with the inverse property may be derived with ease by use of the autotopism group.

Chapter I deals with general loops, Chapter II with I.P. loops (loops with the inverse property), and Chapter III with various problems of construction. In particular, most of our examples connected with the theory of the first two chapters have been deferred until Chapter III. Each chapter is prefaced by a detailed description of its contents. However, the reader must

Presented to the Society, April 29, 1944 and November 25, 1944, under the titles *Quasigroups with the inverseproperty,* and *Quasigroup theory*; received by the editors February 21, 1946.

consult the main body of the paper for definitions and references to the literature.

Perhaps we should reassure the newcomer to the theory of loops by stating that every effort has been put forth to make the paper reasonably self-contained. We have, of course, assumed a certain familiarity with group theory, but most of the loop theory needed in the paper has been carefully and explicitly stated. Moreover, various known theorems have been proved anew by means of the inner mapping group, especially in §3 of Chapter I; but in such cases, careful references have been given to the literature.

CHAPTER I. GENERAL THEORY

This chapter is devoted mainly to a theory of loops without the introduction of special laws. However, we do on occasion study special classes of loops, for example, the finite ones. It has been thought worthwhile to preface the main study (in §1) with some remarks on sets and mappings of sets, and to derive a few theorems on the isotopy problems of groupoids. (In particular we consider a theory of multiplicative ideals which is not applied in the sequel but is of interest in connection with the theory of rings.) Definitions of the terms quasigroup and loop and of certain qualifying adjectives are given in §2.

In §3 we sum up (with references) some of the known results on normal subloops of a loop. The most important contribution of this section is the notion of the inner mapping group $\mathfrak{J}$ of a loop G, the analogue for loops of the inner automorphism group of a group. ($\mathfrak{J}$ does not always consist of automorphisms of G; however a subloop H of G is normal in G if and only if H is mapped into itself by every element of $\mathfrak{J}$.) We use $\mathfrak{J}$ to prove some of the known theorems on normality; and we also show that the *union of an arbitrary collection of normal subloops of a loop G is a normal subloop of G* (Theorem 3G).

In §4 some of the basic properties of the central series of a (nilpotent) group are generalized in an abstract theory of so-called π-series. Here π designates some fixed "characteristic" property of loops, and associated with each π is a class of π-admissible loops, determined by explicit and easily handled postulates, for which the theory is valid. Certain π-admissible loops are called π-nilpotent, and for these the upper and lower π-series exist and have the same (minimal) length. We also give some theorems in this section on a more general class of loops called π-solvable; for example, *the union of all normal π-solvable subloops of a finite π-admissible loop is a* (*uniquely defined*) *normal π-solvable subloop.*

§5 deals briefly with the ϕ-loop of a loop; and §6 considers certain "Lagrange" properties of a finite loop, namely the weak property (L): *the order of every subloop of the finite loop G divides the order of G*, and the strong property (L′): *every subloop H of the finite loop G has property* (L). It is shown in particular that *a finite loop has property* (L′) *if and only if the simple quotient* *loops in its decomposition series have property* (L′). Moreover *every finite loop contains a unique maximal normal subloop with property* (L′).

When π is the property of lying in the centre of the loop G we have the notions of central admissibility, central nilpotency and central solvability. In §7 every loop is shown to be centrally admissible. The various terms in the upper and lower central series are described in detail in terms of the inner mapping group. For finite centrally nilpotent loops G, Theorem 7E and its corollaries give a generalization of the Burnside Basis Theorem for p-groups, which reduces to the usual form when G has prime-power order. Similarly Theorem 7F generalizes a theorem of P. Hall on the order of the automorphism group of a finite p-group. §8 concerns the order of the inner mapping group $\mathfrak{J}$ of a finite centrally nilpotent loop G. It is shown that the order of $\mathfrak{J}$ divides some power of the order of G. (This is remarkable, since there exists a loop of order 5—of course not centrally nilpotent—whose inner mapping group has order $4!=24$.) Moreover it is proved that a finite p-loop G (of order a power of the prime p) is centrally nilpotent if and only if $\mathfrak{J}$ is a p-group. §9 gives a brief discussion of the relation of the theory of finite centrally nilpotent p-loops to P. Hall's work on p-groups.

In §10 the notion of left-associatral series is touched upon lightly; here π is the property of lying in the left-associator (defined in §§1, 2) of the loop G. It is shown that every loop is π-admissible in this sense. Other types of associatral series are also mentioned.

§11 introduces the autotopism group of a groupoid—not to be exploited until Chapter II—and §12 shows the role of the inner mapping group $\mathfrak{J}$ of a finite loop G in the theory of the loop ring of G over a field F. We define two elements x, y of G to be conjugate if and only if $xU=y$ for some element U of $\mathfrak{J}$, and then we may state a theorem wholly analogous to one for group rings: *If F is algebraically closed and* (to specialize slightly) *of characteristic zero, the loop ring of G over F is a direct sum of h simple algebras, where h is the number of distinct classes of conjugate elements of G.*

1. **Groupoids.** It will be convenient to recall some of the terminology of set theory. A mapping T ($a\rightarrow aT$) of a set G into a set H is called *single-valued* if, for every element a of G, aT is a uniquely defined element of H. The single-valued mapping T of G into H is said to be (i) a *one-to-one* mapping of G *into* H if $aT\neq bT$ for every two distinct elements a, b of G and (ii) a *one-to-one* mapping of G *upon* H if (i) holds and, in addition, every element of H has the form aT for some a in G. When T is a one-to-one mapping of G upon H, then to every b of H there exists a unique element $a=bT^{-1}$ of G such that $aT=b$. In this case T^{-1} is a one-to-one mapping of H upon G, called the *inverse* of T. In the sequel a one-to-one mapping P of a set G upon itself will often be called a *permutation* of G.

According to Hausmann and Ore [1][1] a set G is defined to be a *groupoid*

[1] Numbers in brackets refer to the Bibliography at the end of the paper.

relative to an operation $(\cdot)$ if and only if, to every ordered pair a, b of elements of G, there corresponds a uniquely defined element $a\cdot b$ of G. Since a set may be a groupoid relative to more than one operation it is sometimes convenient to speak for example of "the groupoid $G(\cdot)$." If f is any fixed element of a groupoid $G(\cdot)$ we may define two single-valued mappings L_f, R_f of G into itself by

$$aL_f = f\cdot a, \qquad aR_f = a\cdot f, \tag{1.1}$$

where (1.1) is to hold for all a of G. An element 1 of a groupoid $G(\cdot)$ is said to be a unit of $G(\cdot)$ if, for every a of G,

$$a\cdot 1 = 1\cdot a = a. \tag{1.2}$$

If e is also a unit then $e=e\cdot 1=1$, and hence a unit, if it exists, is unique. An element f of $G(\cdot)$ is said to be *left-nonsingular* (*right-nonsingular*) if L_f (R_f) is a permutation of G. (Note that if $G(\cdot)$ consists of the natural numbers $1, 2, \cdots$ under ordinary multiplication, the only left- or right-nonsingular element is the number 1.)

Two groupoids $G(\cdot)$ and $H(o)$ are defined to be *isotopic* if there exist three one-to-one mappings U, V, W (not necessarily distinct) of G upon H such that

$$(x\cdot y)W = (xU)o(yV) \tag{1.3}$$

for all x, y of G. In particular two groupoids $G(*)$ and $H(o)$ are said to be *isomorphic* if there exists a one-to-one mapping T of G upon H such that

$$(x*y)T = (xT)o(yT) \tag{1.4}$$

for all x, y of G. Clearly isotopy and isomorphism are equivalence relations. In particular two isomorphic groupoids are abstractly identical. Finally two groupoids $G(\cdot)$ and $G(*)$, defined upon the same set G, are said to be *principal isotopes* if there exist two permutations P, Q of G such that

$$x\cdot y = (xP)*(yQ) \tag{1.5}$$

for all x, y of G.

Lemma 1A. *Let $G(\cdot)$ and $H(o)$ be isotopic groupoids. Then there exists a groupoid $G(*)$ isomorphic to $H(o)$ and isotopic to $G(\cdot)$. In particular $G(*)$ may be chosen to be a principal isotope of $G(\cdot)$.*

Proof. We may assume (1.3), pick T arbitrarily as a one-to-one mapping of G upon H, and define $G(*)$ by (1.4). It follows at once that $(x\cdot y)W_1 = (xU_1)*(yV_1)$ for all x, y of G, where $U_1=UT^{-1}$, $V_1=VT^{-1}$, $W_1=WT^{-1}$. But U_1, V_1, W_1 are permutations of G. By the special choice $T=W$ we derive (1.5) with $P=UW^{-1}$, $Q=VW^{-1}$.

Thus, as A. A. Albert has pointed out in various papers, if we consider two isomorphic systems as identical then in the theory of isotopy there is no loss of generality in restricting attention to principal isotopes. The following theorem may be proved exactly as in Albert [1], and we shall omit the proof.

THEOREM 1A. *Let $G(\cdot)$ be a groupoid. Then a necessary and sufficient condition that there exist a groupoid $H(o)$, with a unit, isotopic to $G(\cdot)$ is that $G(\cdot)$ possess at least one left-nonsingular element f and at least one right-nonsingular element g. Every principal isotope $G(o)$ of this type is given by*

$$xoy = (xR_g^{-1})\cdot(yL_f^{-1}) \tag{1.6}$$

for some such fixed pair f, g of $G(\cdot)$. In this case the unit of $G(o)$ is $e=f\cdot g$.

If $G(o)$ is given by (1.6), the one-to-one mappings $L_a{}^o$, $R_a{}^o$ of G into itself may be defined by $xL_a{}^o=aox$, $xR_a{}^o=xoa$. Now suppose in particular that $G(\cdot)$ has a unit 1. It follows at once that

$$gR_g^{-1} = 1, \qquad fL_f^{-1} = 1, \tag{1.7}$$

since indeed $1R_g=g$, $1L_f=f$. But, even more important, we have

$$\overset{o}{L}_g = L_f^{-1}, \qquad \overset{o}{R_f} = R_g^{-1}. \tag{1.8}$$

For example, from (1.6), $xL^o{}_g=gox=(gR_g{}^{-1})\cdot(xL_f{}^{-1})=1\cdot(xL_f{}^{-1})=xL_f{}^{-1}$, and so $L^o{}_g=L_f{}^{-1}$. From (1.8) it is clear that g is a left-nonsingular element and that f is a right-nonsingular element of $G(o)$.

COROLLARY TO THEOREM 1A. *Let $G(\cdot)$ be a groupoid with unit 1. Let f, g be respectively a left-nonsingular and a right-nonsingular element of $G(\cdot)$, and let $G(o)$ be the principal isotope, with unit $e=fg$, given by (1.6). Then f, g are respectively a right-nonsingular and a left-nonsingular element of $G(o)$, and we have*

$$x\cdot y = x(R^o{}_f)^{-1}oy(L^o{}_g)^{-1} \tag{1.9}$$

for all x, y of G. Moreover $1=gof$.

Proof. By (1.8) and (1.6) the right-hand side of (1.9) reduces to $[(xR_g)R_g{}^{-1}]\cdot[(yL_f)L_f{}^{-1}]=x\cdot y$. The rest of the proof was given above, save for the point that $gof=gR_g{}^{-1}\cdot fL_f{}^{-1}=1\cdot 1=1$.

It is to be noted that a *subgroupoid* $H(\cdot)$ of a groupoid $G(\cdot)$ is by definition a subset H of G which is a groupoid relative to $(\cdot)$. Again a groupoid $G(\cdot)$ is said to be *semigroup* if

$$(a\cdot b)\cdot c = a\cdot(b\cdot c) \tag{1.10}$$

for all a, b, c of G; that is to say, a semigroup is an associative groupoid. Every groupoid $G(\cdot)$ contains certain associative subgroupoids. If $G(\cdot)$ is any groupoid we define the subsets A_λ, A_μ, A_ρ of G as follows[2]:

[2] These associators and others have been defined by various authors, for example, by Garrison [1].

Definitions. *A_λ is the set of all elements a of $G(\cdot)$ such that*

$$(1.11) \qquad (a\cdot x)\cdot y = a\cdot(x\cdot y)$$

for all x, y of G.

A_μ is the set of all elements a of $G(\cdot)$ such that

$$(1.12) \qquad (x\cdot a)\cdot y = x\cdot(a\cdot y)$$

for all x, y of G.

A_ρ is the set of all elements a of $G(\cdot)$ such that

$$(1.13) \qquad (x\cdot y)\cdot a = x\cdot(y\cdot a)$$

for all x, y of G.

We shall speak of A_λ, A_μ, A_ρ respectively as the left-, middle- and right-associators of $G(\cdot)$.

If a, b are two elements of A_λ, and x, y any elements of $G(\cdot)$, then, by repeated uses of (1.11), $(a\cdot b)\cdot(x\cdot y)=a\cdot[b\cdot(x\cdot y)]=a\cdot[(b\cdot x)\cdot y]=[a\cdot(b\cdot x)]\cdot y =[(a\cdot b)\cdot x]\cdot y$. Thus $a\cdot b$ is in A_λ for all a, b of A_λ, and so A_λ is a subgroupoid of $G(\cdot)$. Again if a, b, c are any three elements of A_λ then by (1.11) with $x=b$, $y=c$ we see that (1.10) holds, and A_λ is a semigroup. Since a similar result holds for A_μ and A_ρ, we have proved the first statement of the following theorem.

Theorem 1B. *If $G(\cdot)$ is any groupoid, each of the three associators $A_\lambda(\cdot)$, $A_\mu(\cdot)$, $A_\rho(\cdot)$ of $G(\cdot)$ is a subgroupoid of $G(\cdot)$ and in fact a semigroup. If $G(\cdot)$ has unit* 1, *and if $G(o)$ is a groupoid with unit, isotopic to $G(\cdot)$, then the three associators $A_\lambda(o)$, $A_\mu(o)$, $A_\rho(o)$ of $G(o)$ are respectively isomorphic to the corresponding associators of $G(\cdot)$.*

Proof. We note that if $G(\cdot)$ has unit 1, then 1 is common to the three associators of $G(\cdot)$ and hence the latter are non-empty. Because of Lemma 1A we may assume that $G(o)$ is the principal isotope of $G(\cdot)$ given by (1.6). First we prove that $A_\lambda(\cdot)$ and $A_\lambda(o)$ are isomorphic. Consider the mapping L of $A_\lambda(\cdot)$ into $G(o)$ given by

$$(1.14) \qquad aL = (a\cdot f)\cdot g,$$

and note that, by (1.11), (1.14) is equivalent to $aL=a\cdot(f\cdot g)=a\cdot e$. If $aL=bL$ for a, b in $A_\lambda(\cdot)$ then $(af)R_g=(bf)R_g$ and so $af=bf$ since g is a right-nonsingular element of $G(\cdot)$. Inasmuch as f is a left-nonsingular element of $G(\cdot)$ the element $h=1L_f^{-1}$ exists and has the property that $fh=1$. But then $a=a\cdot fh =af\cdot h=bf\cdot h=b\cdot fh=b\cdot 1=b$, since a, b are in $A_\lambda(\cdot)$. It follows that $aL=bL$ implies $a=b$. Therefore *L is a one-to-one mapping of $A_\lambda(\cdot)$ into $G(o)$.*

Again, if x is any element of G, a any element of $A(\cdot)$, then

$$(1.15) \qquad (aL)ox = a\cdot x,$$

since $(aL)ox=(aLR_g^{-1})\cdot(xL_f^{-1})=(a\cdot f)\cdot xL_f^{-1}=a\cdot(f\cdot xL_f^{-1})=a\cdot x$. Moreover $[a\cdot xR_g^{-1}]R_g=(a\cdot xR_g^{-1})\cdot g=a\cdot(xR_g^{-1}\cdot g)=a\cdot x$ and so

$$(a\cdot x)R_g^{-1} = a\cdot(xR_g^{-1}) \tag{1.16}$$

for all $a\in A_\lambda(\cdot)$, $x\in G$. Thus, by use of (1.15) and (1.16), $[(aL)ox]oy=(a\cdot x)oy$ $=[(a\cdot x)R_g^{-1}]\cdot(yL_f^{-1})=[a\cdot(xR_g^{-1})]\cdot(yL_f^{-1})=a\cdot[(xR_g^{-1})\cdot(yL_f^{-1})]=a\cdot(xoy)$ $=(aL)o(xoy)$. It follows that

$$[(aL)ox]oy = (aL)o(xoy) \tag{1.17}$$

for all a of $A_\lambda(\cdot)$ and x, y of $G(o)$. Therefore L is a one-to-one mapping of $A_\lambda(\cdot)$ into $A_\lambda(o)$.

If we now observe the relationship between (1.6) and (1.9) it will be clear that *the mapping L_o, defined by*

$$cL_o = (cog)of, \qquad c\in A_\lambda(o), \tag{1.18}$$

is a one-to-one mapping of $A_\lambda(o)$ into $A_\lambda(\cdot)$. If a is any element of $A_\lambda(\cdot)$ then, by (1.18), (1.17), (1.15) and the corollary to Theorem 1A, we see that $(aL)L_o=[(aL)og]of=(aL)o(gof)=a\cdot(gof)=a\cdot 1=a$. Thus since aL is in $A_\lambda(o)$ it follows that L_o is in fact a one-to-one mapping of $A_\lambda(o)$ *upon* $A_\lambda(\cdot)$. Similarly L is a one-to-one mapping of $A_\lambda(\cdot)$ upon $A_\lambda(o)$; and in fact L, L_o are inverse mappings. Finally, if a, b are in $A_\lambda(\cdot)$, then, by (1.15) and the fact that $bL=be$, $(aL)o(bL)=a\cdot(bL)=a\cdot be=ab\cdot e=(ab)L$, or $(ab)L=(aL)o(bL)$. Hence $A_\lambda(\cdot)$ and $A_\lambda(o)$ are isomorphic, as was to be proven.

Similar proofs may be given to show that the mappings M, R, defined by

$$xM = f\cdot(x\cdot g) \tag{1.19}$$

and

$$xR = f\cdot(g\cdot x) \tag{1.20}$$

induce isomorphicms respectively of $A_\mu(\cdot)$ upon $A_\mu(o)$ and of $A_\rho(\cdot)$ upon $A_\rho(o)$. A slight difficulty arises however in the proof of the fact that

$$[xo(aM)]oy = xo[(aM)oy] \tag{1.21}$$

for all a of $A_\mu(\cdot)$ and x, y of G, and we therefore give this in detail: $xo(aM)=(xR_g^{-1})$. $[(f\cdot ag)L_f^{-1}]=(xR_g^{-1})\cdot(a\cdot g)=[(xR_g^{-1})\cdot a]\cdot g$, and hence $[xo(aM)]oy = [xR_g^{-1}\cdot a]\cdot(yL_f^{-1}) = (xR_g^{-1})\cdot[a\cdot(yL_f^{-1})]= xo[\{a(yL_f^{-1})\}L_f]$ $=xo[(f\cdot a)\cdot yL_f^{-1})]=xo[\{(f\cdot a)\cdot g\}oy]=xo[(aM)oy]$.

An element a of a groupoid $G(\cdot)$ which is both left- and right-nonsingular will be said to be *nonsingular.*

LEMMA 1B. *If $G(\cdot)$ is a semigroup with unit* 1, *every left-nonsingular (right-nonsingular) element of $G(\cdot)$ is nonsingular. Moreover the set H of all nonsingular elements is a subsemigroup of $G(\cdot)$ and in fact a group.*

Proof. If f is left-nonsingular, let $f^{-1}=1L_f^{-1}$ so that $f\cdot f^{-1}=1$. Then $(f^{-1}\cdot f)L_f=f\cdot(f^{-1}\cdot f)=(f\cdot f^{-1})\cdot f=1\cdot f=f$; that is, $f^{-1}\cdot f=fL_f^{-1}=1$. If x is any element of $G(\cdot)$ the element $y=xR_{f^{-1}}$ has the property that $yR_f=(x\cdot f^{-1})\cdot f=x\cdot(f^{-1}\cdot f)=x\cdot 1=x$; conversely if $yR_f=x$ then $xR_{f^{-1}}=y\cdot(f\cdot f^{-1})=y$. Hence $R_f^{-1}=R_{f^{-1}}$, and similarly $L_f^{-1}=L_{f^{-1}}$; in particular both f and f^{-1} are nonsingular. Similarly if g is right-nonsingular and if $g^{-1}=1R_g^{-1}$ then $L_g^{-1}=L_{g^{-1}}$, $R_g^{-1}=R_{g^{-1}}$, and both g and g^{-1} are nonsingular. Finally, if p, q are nonsingular then $xR_{pq}=x\cdot pq=xp\cdot q=xR_pR_q$ and $R_{pq}^{-1}=R_q^{-1}R_p^{-1}$; pq is right-nonsingular and so nonsingular. This essentially proves that $H(\cdot)$ is a group.

We may now prove the analogue of another theorem due to Albert [1].

THEOREM 1C. *Let $G(\cdot)$ be a semigroup with unit 1. Then any groupoid $H(o)$ with a unit which is isotopic to $G(\cdot)$ is in fact isomorphic to $G(\cdot)$, and hence in particular is a semigroup.*

Proof. As before we may assume that $H(o)$ is the principal isotope $G(o)$ given by (1.6). Since $G(\cdot)$ is a semigroup, $A_\lambda(\cdot)$ coincides with $G(\cdot)$, and the mapping L defined by (1.14), or by $aL=a\cdot(f\cdot g)$, gives an isomorphism of $A_\lambda(\cdot)$ upon $A_\lambda(o)$. By Lemma 1B, $e=f\cdot g$ is a nonsingular element of $G(\cdot)$ and hence $L=R_e$ is a permutation of G. It follows that $A_\lambda(o)$ coincides with $G(o)$.

If $G(\cdot)$ is a groupoid, the set $A=A_\lambda\cap A_\mu\cap A_\rho$ consisting of all elements common to $A_\lambda(\cdot)$, $A_\mu(\cdot)$ and $A_\rho(\cdot)$ may be called the *associator*. Clearly $A(\cdot)$ is a subgroupoid of $G(\cdot)$ and in fact a semigroup. The question is still open as to whether isotopic groupoids with units have isomorphic associators A. *Added in proof*: Since this was written I have constructed simple counter-examples.

The subset $C(\cdot)$ of a groupoid $G(\cdot)$, consisting of those elements a of A such that $a\cdot x=x\cdot a$ for all x of G, is called the centre of $G(\cdot)$. More loosely stated, $C(\cdot)$ consists of all elements of $G(\cdot)$ which commute and associate with the elements of $G(\cdot)$. Theorem 1 D is also essentially Albert's[3].

THEOREM 1D. *The centre $C(\cdot)$ of a groupoid $G(\cdot)$ is an associative subgroupoid of $G(\cdot)$. If $G(\cdot)$ has a unit, and if $G(o)$ is a groupoid with unit, isotopic to $G(\cdot)$, then the centre $C(o)$ of $G(o)$ is isomorphic to $C(\cdot)$.*

Proof. The proof follows the pattern of previous proofs. The reader may prove the first statement. The essential point in regard to the second statement is the fact that if a is in $C(\cdot)$ then $aL=aM=aR=a\cdot e$, where L, M, R are given by (1.14), (1.19) and (1.20) respectively, and where $e=f\cdot g$. Hence L, M and R may be shown to yield the same isomorphism of $C(\cdot)$ upon $C(o)$, where $G(o)$ is assumed to be given by (1.6). It should moreover be obvious from this remark where the difficulty lies in regard to a like theorem about $A(\cdot)$.

An *automorphism* S of a groupoid $G(\cdot)$ is a one-to-one mapping of G upon itself such that

$$(x\cdot y)S = (xS)\cdot(yS) \tag{1.22}$$

for all x, y of G. Following R. Baer [3] and the obvious suggestion from group theory we shall define a subset H of $G(\cdot)$ to be *characteristic* if $HS \leqq H$ (that is, if hS is in H for every h of H) for every automorphism S of $G(\cdot)$. An *endomorphism* S of a groupoid $G(\cdot)$ is a single-valued mapping S of G into or upon itself such that (1.22) holds for all x, y of $G(\cdot)$; and a subset H of $G(\cdot)$ will be called *fully characteristic* (Baer) if $HS \leqq H$ for every endomorphism of $G(\cdot)$.

Theorem 1E. *If $G(\cdot)$ is a groupoid, the subgroupoids $A_\lambda(\cdot)$, $A_\mu(\cdot)$, $A_\rho(\cdot)$, $A(\cdot)$ and $C(\cdot)$, defined above, are all characteristic.*

Proof. Let a be any element of $A_\lambda(\cdot)$, S any automorphism of $G(\cdot)$. Then, for all x, y of G, $[(aS)\cdot x]\cdot y = \{[a\cdot(xS^{-1})]\cdot(yS^{-1})\}S = \{a\cdot[(xS^{-1})\cdot(yS^{-1})]\}S = (aS)\cdot(x\cdot y)$, and hence aS is in $A_\lambda(\cdot)$. Thus $A_\lambda(\cdot)$ is characteristic, and similarly for $A_\mu(\cdot)$, $A_\rho(\cdot)$. If a is in $A(\cdot)$, aS is then in each of $A_\lambda(\cdot)$, $A_\mu(\cdot)$ and $A_\rho(\cdot)$, and so in $A(\cdot)$. Finally if a is in $C(\cdot)$, $(aS)\cdot x = [a\cdot(xS^{-1})]S = [(xS^{-1})\cdot a]S = x\cdot(aS)$. Hence aS is an element of the characteristic groupoid $A(\cdot)$ which commutes with every element of $G(\cdot)$, and so aS is in $C(\cdot)$.

As we shall show in the next section, all of the above theorems are valid for loops. Indeed they also hold, with obvious modifications, for various types of rings (see for example [Albert 3]). The following notion of a multiplicative ideal stems from ring theory, and apparently has little value for the theory of loops.

Definition. *A subset H of a groupoid $G(\cdot)$ will be said to be a left ideal, a right ideal, or an ideal of $G(\cdot)$ according as it satisfies the first two, the last two, or all of the following conditions:*

(i) *For every a of H and x of $G(\cdot)$, $x\cdot a$ is in H.*

(ii) *For every a of H and every left-nonsingular f of $G(\cdot)$, aL_f^{-1} is in H.*

(iii) *For every a of H and x of $G(\cdot)$, $a\cdot x$ is in H.*

(iv) *For every a of H and every right-nonsingular g of $G(\cdot)$, aR_g^{-1} is in H.*

Every ideal of $G(\cdot)$ is a left ideal (and a right ideal) but not always conversely. Moreover, left, right and two-sided ideals are clearly subgroupoids of $G(\cdot)$.

Theorem 1F. *Let $G(\cdot)$ be a groupoid, $H(\cdot)$ any left (right, two-sided) ideal of $G(\cdot)$. Moreover let $G(\cdot)$ possess an isotope $Q(o)$ with a unit. Then $Q(o)$ possesses a left (right, two-sided) ideal $K(o)$ whose elements are in one-to-one correspondence with those of H. If $H(\cdot)$ satisfies both* (ii) *and* (iv) *above, then $K(o)$ is isotopic to $H(\cdot)$.*

Corollary. *If $G(\cdot)$, $Q(o)$ are isotopic groupoids, each with a unit, then their (two-sided) ideals are isotopic in pairs.*

Proof. Again assume that $Q(o)=G(o)$ where the latter is given by (1.6). It follows at once, by (ii) and (i), that H forms a left ideal $H(o)$ of $G(o)$. In fact if $a\in H$ then $aL_f^{-1}=b\in H$ and so $xoa=xR_g^{-1}\cdot b\in H$ for all x of G. Moreover the identity mapping sets up a one-to-one correspondence between the elements of $H(o)$ and $H(\cdot)$. If $H(\cdot)$ satisfies (iv) as well as (ii), then both L_f^{-1} and R_g^{-1} are permutations of H as well as of G, and (1.6) immediately yields the fact that the groupoids $H(\cdot)$ and $H(o)$ are isotopes. This completes the proof for left ideals, and the other cases give no trouble. The corollary is immediate.

It should perhaps be pointed out that in the theory of linear algebras (of finite order over a field) we consider only those ideals (in the present sense) which form a group under addition. But then condition (ii) is a consequence of (i), and (iv) a consequence of (iii).

Since we have been preoccupied in this section with isotopic systems it has seemed worthwhile to put up with the nuisance of emphasizing the operations $((\cdot)$, (o) or $(*))$ of the various systems under consideration. In most of what follows we shall usually assume that the operation in question is $(\cdot)$. Moreover we shall often write xy for $x\cdot y$, $xy\cdot z$ for $(z\cdot y)\cdot z$, and so forth.

2. **Quasigroups and loops.** The main purpose of this section is to list for ready reference the definitions of quasigroup and loop and of certain important subsets of the latter. The only novelty in these definitions is the restricted meaning given to the term *abelian*. We also give slightly improved analogues for loops of the theorems of the preceding section.

In terms of the language of §1 a *quasigroup* G might be defined to be a groupoid in which every element x is nonsingular. More explicitly a set G is a quasigroup if and only if the following two laws are satisfied.

I. *To every ordered pair x, y of elements of G there corresponds a unique element xy of G, called their product.*

II. *If, in the equation $xy=z$, any two of the symbols x, y, z are assigned as elements of G, the third is uniquely determined as an element of G.*

Clearly a groupoid is a set in which only (I) is assumed.

A *loop* is a quasigroup with a unit element. Thus a loop G obeys (I), (II) and the following.

III. *There exists an element* 1 *of G with the property that* $1\cdot x=x\cdot 1=x$ *for every x of G.*

A loop G can have exactly one unit. Moreover if a subset H of G obeys (I) and (II), with respect to the operation $(\cdot)$ of G, then it will contain the unit 1 of G. Such a subset we call a *subloop*. The *order* of a loop is by definition its cardinal number. An infinite loop may contain subgroupoids (subsets obeying (I)) which are not subloops, but we shall ignore these in the sequel. A *proper* subloop is one which neither coincides with G nor contains only the element 1.

An *associative* loop G is one which obeys:

IV. *For every triple x, y, z of G, $xy\cdot z=x\cdot yz$.*
Such a loop is of course a group, and we shall use the terms "group" and "associative loop" interchangeably.

A commutative loop G is one subject to the following law.

V. *For every two elements x, y of G, $xy=yx$.*

We define a loop G to be *abelian* if and only if all five of the above laws hold. Thus for the purposes of the present paper the terms "abelian loop" and "abelian group" are synonymous. It is important to note that writers on quasigroup theory (including the present author) have frequently used "abelian" as equivalent to "commutative," in contrast with the present usage. We might also remind the reader that laws (I), (II), and (IV) together imply (III); an associative quasigroup is a group.

Since every loop is a groupoid, all of the theorems and definitions of §1 may be applied immediately to loops. However, Theorem 1F has little interest, since no ideal which is a subloop of a loop can be a proper subloop. It is easily verified (and we take this for granted) that every groupoid isotopic to a loop is a quasigroup.

THEOREM 2A. *If G is any loop, each of the subsets A_λ, A_μ, A_ρ, A and C of G (as defined in §1) is a characteristic associative subloop of G. Moreover A_λ, A_μ, A_ρ and C are respectively isomorphic to the corresponding entities defined for any loop isotopic to G.*

COROLLARY. *Every loop isotopic to a group is an isomorphic group.*

Proof. The only new point at issue is to show that A_λ (for example) is not only a semigroup but a group. This might appear to follow directly from Lemma 1B, since every element x of a loop is nonsingular; however, we must show that if $a\in A_\lambda$ then L_a^{-1} and R_a^{-1} are permutations not only of G but of A_λ. If a is in A_λ, write $a^{-1}=1L_a^{-1}$, so that $aa^{-1}=1$. Then for all x, y in G we have $a(a^{-1}x\cdot y)=(a\cdot a^{-1}x)y=(aa^{-1}\cdot x)y=xy=aa^{-1}\cdot xy=a(a^{-1}\cdot xy)$; and so $a^{-1}x\cdot y=a^{-1}\cdot xy$, a^{-1} is in A_λ. As in the proof of Lemma 1B, we may now show that $L_a^{-1}=L_{a^{-1}}$, $R_a^{-1}=R_{a^{-1}}$. At this stage Lemma 1B may be applied to show that A_λ is a group. A similar proof may be used in the case of A_ρ, but A_μ requires special handling. If $a\in A_\mu$ we define $a^{-1}=1L_a^{-1}$ as before, so that $aa^{-1}=1$. Thus for every x in G, $xa\cdot a^{-1}=x\cdot aa^{-1}=x$, whence $R_{a^{-1}}=R_a^{-1}$ and, in particular, $a^{-1}a=1$. A similar calculation now gives $L_{a^{-1}}=L_a^{-1}$. Finally, if x, y are in G we set $z=yL_a^{-1}$, so that $y=az$, and derive $xa^{-1}\cdot y=xa^{-1}\cdot az=(xa^{-1}\cdot a)z=xz=x(a^{-1}\cdot az)=x\cdot a^{-1}y$. It follows that a^{-1} is in A_μ, and the proof may readily be completed.

3. **Normality for loops. The inner mapping group.** A single-valued mapping T of a loop G upon (into) a loop K is said to be a *homomorphism of G upon (into)* the loop K if and only if

$$(xy)T = (xT)(yT) \tag{3.1}$$

for all x, y of G. Moreover, G is said to be *homomorphic with* (*with a subloop of*) K, and the loop GT consisting of all xT with x in G is said to be the *map* or *homomorph* of G under T. (Clearly G is homomorphic with GT for any homomorphism T of G.) In the notation of R. Baer [3] the subloop H of G consisting of all x such that $xT=1T$ is called the *kernel* of T.

DEFINITION. A subloop H of a loop G is a *normal* subloop of G if and only if H is the kernel of some homomorphism of G.

A. A. Albert [1, 2] and M. F. Smiley [1] have given necessary and sufficient conditions that a subloop H be normal. (We shall derive an equivalent condition below.) Moreover, these authors and Baer, particularly the latter, have developed an extensive theory of normal subloops, wholly analogous to the corresponding theory for groups. It will be convenient to list some of their theorems without proof, and we shall do so, but our main purpose here is to develop an analogue for loops of the inner automorphism group of a group. In some cases this "inner mapping group" $\mathfrak{J}$ facilitates brief proofs of known results. It also leads to one theorem which seems to be new (Theorem 3G).

LEMMA 3A. *If H is a subloop of a loop G, the following condition is necessary and sufficient that H be normal in G: Let x, y be arbitrary but fixed elements of G; then, in the equation*

$$h_1x\cdot h_2y = h_3\cdot xy, \tag{3.2}$$

whenever two of h_1, h_2, h_3 are assigned as elements of H the third is uniquely determined as an element of H.

Proof. (i) *Sufficiency*[3]. Suppose that the subloop H satisfies the condition of Lemma 3A, and designate by Hx the set of all elements hx with h in H. From (3.2) with $x=1$ (the unit of G) we see that *any element of a* "coset" *Hy determines the same coset.* Moreover for any elements x, y of G,

$$Hx\cdot Hy = H\cdot xy. \tag{3.3}$$

If x, z are given, and if y is the unique solution of the equation $xy=z$, it follows from (3.2) that *a necessary and sufficient condition that $Hx\cdot u=Hz$ for an element u of G is that $u\in Hy$.* Similarly if y, z are given and if x is determined by $xy=z$, it follows that *a necessary and sufficient condition that $v\cdot Hy=Hz$ for an element v of G is that $v\in Hx$.* Therefore the set G/H consisting of all the distinct cosets Hx is a quasigroup. Moreover, by (3.3), the single-valued mapping T defined by $xT=Hx$ is a homomorphism of G, and $xT=1T$ if and only if $Hx=H$ or $x\in H$. Thus H is a normal subloop of G.

(ii) *Necessity*. Let H be the kernel of a homomorphism T of G. If $xT=yT$, let $u=yR_x^{-1}$. Then $ux=y$, $uT\cdot xT=yT=xT=1T\cdot xT$, $uT=1T$, $u\in H$. But

[3] The method used in this proof is essentially that of Smiley [1].

conversely if $u \in H$ then $(ux)T = uT \cdot xT = 1T \cdot xT = xT$. Hence the coset Hx consists of exactly those elements y for which $yT = xT$. The rest of the proof is an obvious consequence of this fact and (3.1).

In this proof we have incidentally encountered the notion of a quotient loop G/H. The following theorem is obvious:

THEOREM 3A. *Let H be the kernel of a homomorphism T of a loop G. Then the quotient loop G/H is isomorphic to the homomorph GT under the mapping $Hx \rightarrow xT$.*

From (3.2) with $h_2 = 1$ we derive $h_1 R_x R_y = h_3 R_{xy}$, or $h_1 R_{x,y} = h_3$, where

$$R_{x,y} = R_x R_y R_{xy}^{-1}. \tag{3.4}$$

Again from (3.2) with $h_1 = 1$ we derive $h_2 R_y L_x = h_3 R_{xy}$ or $h_2 M_{x,y} = h_3$, where

$$M_{x,y} = R_y L_x R_{xy}^{-1}. \tag{3.5}$$

Thus the following is an immediate consequence of Lemma 3A.

LEMMA 3B. *A necessary condition that a subloop H of a loop G should be normal in G is that H be mapped into itself by all the permutations $R_{x,y}$, $M_{x,y}$ and their inverses.*

We say of course that H is mapped into itself by a mapping S of G if $hS \in H$ for every h of H. It would be fairly easy to show at this stage that the condition of Lemma 3B is also sufficient, but we shall do this more elegantly later.

DEFINITIONS. *If G is a loop, let $\mathfrak{G}$ be the permutation group consisting of the permutations R_x, R_x^{-1}, L_x, L_x^{-1} for all x in G, and of all products of a finite number of these. We shall call $\mathfrak{G}$*[4] *the group associated with G.*

Let $\mathfrak{I} \leqq \mathfrak{G}$ be the subgroup generated by the set of all permutations $R_{x,y}$, $M_{x,y}$ with x, y in G. We shall call $\mathfrak{I}$ the inner mapping group of G.

THEOREM 3B. *Let G be a loop, $\mathfrak{G}$ its associated group, and $\mathfrak{I}$ its inner mapping group. Then $1U = 1$ for every element of $\mathfrak{I}$, where 1 is the unit of G. Moreover every element X of $\mathfrak{G}$ has a unique representation $X = UR_x$ where U is in $\mathfrak{I}$ and (hence) $x = 1X$.*

COROLLARY 1. *A necessary and sufficient condition that an element T of $\mathfrak{G}$ be in $\mathfrak{I}$ is that $1T = 1$.*

COROLLARY 2. *Every element X of $\mathfrak{G}$ has a unique representation $X = VL_x$ where V is in $\mathfrak{I}$ and (hence) $x = 1X$.*

COROLLARY 3. *If a is in G, X in $\mathfrak{G}$, then $aX = aU \cdot x = x \cdot aV$ where U, V are in $\mathfrak{I}$ and $x = 1X$.*

[4] This is Albert's group G_T (Albert [1, 2]).

COROLLARY 4. *If G is a finite loop, $G:1=\mathfrak{G}:\mathfrak{J}$. In other words, the order of G is the index of $\mathfrak{J}$ in $\mathfrak{G}$.*

Remark. The suggestion implied in Corollary 3 is frequently useful. For example if $b=[r(ap\cdot q)]L_s^{-1}$ it may be important to know that $b=aU\cdot x=x\cdot aV$ where $x=(r\cdot pq)L_s^{-1}$ and where U, V are in $\mathfrak{J}$. In many cases we have little interest in the exact determination of U and V.

Proof. From (3.4) we see that $1R_{x,y}=(xy)R_{xy}^{-1}=1$, and then also that $1=1R_{x,y}^{-1}$. Similarly $1M_{x,y}=(xy)R_{xy}^{-1}=1$ and $1=1M_{x,y}^{-1}$. Since the set consisting of the $R_{x,y}$, $M_{x,y}$ and their inverses generates $\mathfrak{J}$, $1U=1$ for every U of $\mathfrak{J}$. Thus if $X=UR_x$ where U is in $\mathfrak{J}$ we have $1X=1R_x=x$, so that x is uniquely defined. Moreover $U=XR_x^{-1}$, and so U is also unique. It remains to show that every X of G has at least one representation UR_x with U in $\mathfrak{J}$, and this we proceed to do by means of the seven identities which follow:

$$(3.6)\qquad \begin{array}{rrcll}
\text{(i)} & R_xR_y & = & R_{x,y}\cdot R_{xy}; & \\
\text{(ii)} & R_xL_y & = & M_{y,x}\cdot R_{yx}; & \\
\text{(iii)} & R_xR_y^{-1} & = & R_{p,y}^{-1}\cdot R_p, & \text{where } p = xR_y^{-1};\\
\text{(iv)} & R_xL_y^{-1} & = & M_{y,q}^{-1}\cdot R_q, & \text{where } q = xL_y^{-1};\\
\text{(v)} & L_x & = & M_{x,1}\cdot R_x; & \\
\text{(vi)} & R_x^{-1} & = & R_{u,x}^{-1}\cdot R_u, & \text{where } u = 1R_x^{-1};\\
\text{(vii)} & L_x^{-1} & = & M_{x,v}^{-1}\cdot R_v, & \text{where } v = 1L_x^{-1}.
\end{array}$$

These are all readily verified. For example, consider (iii). If $p=xR_y^{-1}$ then $py=x$ and so $R_{p,y}=R_pR_yR_x^{-1}$, or $R_{p,y}^{-1}=R_xR_y^{-1}R_p^{-1}$, or $R_xR_y^{-1}=R_{p,y}^{-1}\cdot R_p$. Note moreover that the last three come from (ii), (iii) and (iv) with $x=1$.

It follows from the definition of $\mathfrak{G}$ that each element X of $\mathfrak{G}$ has at least one representation of form

$$(3.7)\qquad X = X_1X_2\cdots X_r$$

where $r\geqq 1$ is a finite integer, and where each X_i has one of the forms R_x, L_x, R_x^{-1}, L_x^{-1}. For X's with $r=1$ the theorem is immediate in view of (v), (vi) and (vii). Thus we assume inductively that it has been proved for all products (3.7) with less than r factors; then $X=VR_x\cdot X_r$ where $V\in\mathfrak{J}$, $x\in G$, and where X_r has one of the four types just mentioned. In each case we have $R_xX_r=WR_z$ by (3.6), with $W\in\mathfrak{J}$, $z\in G$. Therefore finally $X=VWR_z=UR_z$ with $U\in\mathfrak{J}$, and the induction is complete. This demonstrates the truth of Theorem 3B. Corollary 1 is obvious. As to Corollary 2, if $1X=x$, set $V=XL_x^{-1}$. Then $1V=xL_x^{-1}=1$, so V is in $\mathfrak{J}$; and moreover $X=VL_x$. Corollary 3 then follows from Theorem 3B and from Corollary 2. As to Corollary 4, we deduce from the theorem that each coset $\mathfrak{J}X$ of the subgroup $\mathfrak{J}$ of $\mathfrak{G}$ determines a unique element x of G such that $\mathfrak{J}X=\mathfrak{J}R_x$; thus the number of distinct cosets is equal to the order of G. (It is moreover clear that Corollary 4 holds in a sense even for infinite loops.)

THEOREM 3C. *Let G be loop, $\mathfrak{J}$ the inner mapping group of G. Then a necessary and sufficient condition that a subloop H of G should be normal in G is that H be mapped into itself by $\mathfrak{J}$. (In symbols, $H\mathfrak{J} \leqq H$.)*

Proof. Necessity follows from Lemma 3B and the definition of $\mathfrak{J}$. As to sufficiency, we need merely verify the condition (3.2) of Lemma 3A, and we shall do this by repeated use of Corollary 3 to Theorem 3B. Let x, y be arbitrary but fixed elements of G. Then if h_1, h_2 are any two elements of G, not necessarily in H, we have $h_1x \cdot h_2y = h_1U \cdot (x \cdot h_2y) = (h_1U) \cdot (h_2V \cdot xy) = (h_1UW \cdot h_2V) \cdot xy$, where U, V, W are in $\mathfrak{J}$ and are independent of h_1. (In particular $W^{-1} = R_{h_2V, xy}$.) Thus equation (3.2) may be written as $h_1UW \cdot h_2V = h_3$. If h_2 is in H, so is h_2V, and then h_1UW (or h_1) is in H if and only if h_3 is. Similarly $h_1x \cdot h_2y = h_2U \cdot (h_1x \cdot y) = h_2U \cdot (h_1V \cdot xy)$ $(h_2UW \cdot h_1V) \cdot xy$ for suitable U, V, W independent of h_2, and thus if $h_1 \in H$ we see that $h_2 \in H$ if and only if $h_3 \in H$. This completes the proof.

Remarks. (i) *We have defined $\mathfrak{J}$ to be the group generated by the set of all permutations $R_{x,y}$ and $M_{x,y}$. But the set of all permutations*

$$L_{x,y} = L_xL_yL_{yx}^{-1} \tag{3.8}$$

and

$$N_{x,y} = L_yR_xL_{yx}^{-1} \tag{3.9}$$

may also be shown to generate $\mathfrak{J}$; and finally the set consisting of all the permutations $R_{x,y}$, $L_{x,y}$ and

$$T_x = R_xL_x^{-1} \tag{3.10}$$

is another generating set. (We omit the proof of these easily proved statements.)

(ii) *When G is a group, every element of $\mathfrak{G}$ has the form R_xL_y. Since $1R_xL_y = yx$ we see that $\mathfrak{J}$ consists of the elements $R_xL_x^{-1}$. Thus $\mathfrak{J}$ reduces to the group of inner automorphisms of G, as might have been expected.*

(iii) *There exist non-associative loops G for which $\mathfrak{J}$ is a group of automorphisms, and others for which this is not the case.* (See Chapters II, III.)

(iv) *In any problem concerning normality it is clearly always permissible to work not with all of $\mathfrak{J}$ but merely with any set $\mathfrak{S}$ of generators of $\mathfrak{J}$.* (We shall occasionally use this fact in later sections.)

THEOREM 3D. (i) *The centre C of a loop G is the set of all a of G for which $a\mathfrak{J} = a$ (by which we mean that $aU = a$ for every U of $\mathfrak{J}$).* (ii) *If $a\mathfrak{J} = a$, $x \in G$, $T \in \mathfrak{G}$, then $(ax)T = a \cdot xT$.*

COROLLARY 1. *C is a normal subloop of G.*

COROLLARY 2. *If* $a \in C$, $x \in G$, $T \in \mathfrak{G}$, *then* $(ax)T = a \cdot xT$.

Proof. Let a, x, y be elements of G, with $a\mathfrak{J} = a$. Then $(ax)R_y = ax \cdot y = aU \cdot xy = a \cdot xR_y$, and hence $(a \cdot xR_y^{-1})R_y = a \cdot xR_y^{-1}R_y = ax$ or $(ax)R_y^{-1} = a \cdot xR_y^{-1}$. Similarly $(ax)L_y = a \cdot xL_y$ and $(ax)L_y^{-1} = a \cdot xL_y^{-1}$. Since $\mathfrak{G}$ is generated by the R_y, L_y and their inverses, we have proved (ii). With the same hypothesis on a we have

$$ax = xa \tag{3.11}$$

for all x of G, since $xa = aU \cdot x = x$ for some $U \in \mathfrak{J}$. Moreover the equations

$$ax \cdot y = a \cdot xy, \qquad xa \cdot y = x \cdot ay, \qquad xy \cdot a = x \cdot ya \tag{3.12}$$

hold for all x, y of G, since, by (ii) and (3.11), both sides of each equation can be replaced by $a \cdot xy$. But equations (3.11), (3.12) state that a is in C, according to the definition given in §1. If conversely a satisfies (3.11), (3.12) for all x, y of G, the first equation of (3.12) may be written as $aR_{x,y} = a$ and as $a = aR_{x,y}^{-1}$. Moreover the second equation, by virtue of (3.11), may be rewritten as $ax \cdot y = x \cdot ay$, whence $x \cdot ay = ax \cdot y = a \cdot xy$ or $aM_{x,y} = a$ and $a = aM_{x,y}^{-1}$. Since $\mathfrak{J}$ is generated by the $R_{x,y}$, the $M_{x,y}$ and their inverses, we have $a\mathfrak{J} = a$ for every element a of C. This proves (i).

Corollary 2 is an immediate consequence of Theorem 3D, but for Corollary 1 we must give the proof, hitherto omitted, that C is a group. Let a, b be any two elements of C. Then for every U of $\mathfrak{J}$, $(ab)U = a \cdot bU = ab$, or $(ab)\mathfrak{J} = ab$. Again if $ax = b$ then $ax = b\mathfrak{J} = (ax)\mathfrak{J} = a \cdot x\mathfrak{J}$, so $x = x\mathfrak{J} \in C$. Since $ax = xa$, C is a subloop of G, and it follows from (3.11), (3.12) that C is in fact an abelian group. Corollary 1 now follows at once.

DEFINITION. *If A, B are subloops of a loop G, then $A \cap B$, the set consisting of all elements of G which are common to A and B, is called the intersection of A and B.*

The definition may clearly be extended to any finite or infinite set of subloops of a loop. Such an intersection is readily shown to be a loop (compare the first sentence in the proof of the theorem which follows).

THEOREM 3E[5]. *Let Ω be any set of normal subloops K of a loop G, and let D be the intersection of all the K's of Ω. Then D is a normal subloop of G.*

Proof. If, in the equation $xy = z$, two of x, y, z are given as elements of D, the third is a uniquely determined element common to all the K's and hence in D. Moreover $D\mathfrak{J}$ is in all the K's and hence in D.

DEFINITIONS. If Σ is a set of subsets S of a loop G, the smallest subloop of G which contains each S of Σ (that is, the intersection of all subloops which contain each S of Σ) is designated by $\{\Sigma\}$. Frequently $\{\Sigma\}$ is termed the

[5] Smiley [1]. For Ω finite this was previously proved by Albert [2].

subloop generated by Σ, or by the subsets S of Σ.

If A, B are subloops of a loop G, $\{A, B\}$ is termed the union of A and B. This definition may also be extended to any finite or infinite set of subloops of G.

THEOREM 3F[6]. *If H, K are normal subloops of G then $\{H, K\}$ is a normal subloop of G and $\{H, K\} = HK = KH$, where HK is the set of all hk with $h \in H$, $k \in K$.*

The proof of this theorem by the present methods is brief but not very elegant; hence we omit it. The result extends of course to the union of any finite number of normal subloops, and from this fact we deduce the following theorem which appears to be new for loops.

THEOREM 3G. *Let Σ be any set of normal subloops K of a loop G. Let S be the set of all elements of G contained in one or more unions of a finite number of K's of G. Then S is a normal subloop of G; and in particular S is the union of all the K's of Σ.*

COROLLARY. *The union of any set of normal subloops of a loop G is a normal subloop of G.*

Proof. Clearly S contains every K of Σ, and is contained in the union of the K's. If a is in S then a is in some union P of a finite number of K's. But P is a normal subloop of G, and $P \leqq S$. In particular $a\mathfrak{J} \leqq P\mathfrak{J} \leqq P \leqq S$, and so $S\mathfrak{J} \leqq S$. It now follows that S will be both a normal subloop and the union of all the K's, provided only S is a subloop of G. If also $b \in S$ then $b \in Q$ and $a, b \in PQ = R$, where Q, R are both "finite" unions and thus both in S, both normal subloops of G. Clearly ab and the solutions x, y of $ax = b$, $ya = b$ are in R and hence in S. Thus S is a loop and the proof is complete. It should perhaps be noted that we have leaned somewhat heavily upon the axiom of choice.

Remark. In the process of determining the inner mapping group $\mathfrak{J} = \mathfrak{J}(G)$ of a loop G we introduced the notion of the group $\mathfrak{G}$ associated with a loop G. If B is an abstract loop isomorphic to a subloop A of G, it is readily verified that $\mathfrak{B}$ is a homomorph of the subgroup $\mathfrak{A}$ of $\mathfrak{G}$ generated by the set of all permutations L_a, R_a of G with a in A. Thus in particular we may always consider the inner mapping group $\mathfrak{J}(A)$ of a subloop A of a loop G to be a subgroup of the group $\mathfrak{J} = \mathfrak{J}(G)$.

THEOREM 3H. *Let K be a subloop and H a normal subloop of a loop G. Then $D = H \cap K$ is a normal subloop of K.*

COROLLARY. *If, in addition, H is a subloop of K, then H is normal in K.*

Proof. As remarked earlier, D is a subloop of G and hence of K. Also

[6] Albert [2, Theorem 3], Smiley [1, Theorem 4], Baer [3, Theorem 1].

$D\cdot\mathfrak{J}(K)\leqq H\cdot\mathfrak{J}(K)\leqq H$, so $D\cdot\mathfrak{J}(K)\leqq(H\cap K)=D$. In the case of the corollary, $D=H$.

THEOREM 3I[7]. *If H is a normal subloop of $\{H, K\}$ for K a subloop of the loop G, then $\{H, K\}=HK=KH$, and reciprocal isomorphisms between $(HK)/H$ and $K/(H\cap K)$ are obtained by mapping the coset X of $(HK)/H$ upon the set $X\cap K$ and by mapping the coset Y of $K/(H\cap K)$ upon the set HY.*

A proof by the present method would be exceedingly awkward. The normality of $H\cap K$ in K follows from Theorem 3H.

THEOREM 3J. *Let H, K, L be subloops of a loop G, and let K be a normal subloop of L. Then $H\cap K$ is a normal subloop of $H\cap L$.*

Proof. Write $A=H\cap K$, $B=H\cap L$, $\mathfrak{M}=\mathfrak{J}(B)$. We may assume, by the preceding remark, that $\mathfrak{M}\leqq\mathfrak{J}(H)\cap\mathfrak{J}(L)$. Then $A\mathfrak{M}\leqq H\mathfrak{M}\leqq H$ and $A\mathfrak{M}\leqq K\mathfrak{M}\leqq K$, so $A\mathfrak{M}\leqq(H\cap K)=A$.

The following theorem, for which we shall have frequent use, is very often taken for granted in the literature. We shall omit the proof, merely remarking that this can be given most neatly by the methods of Baer [3][8].

THEOREM 3K. *Let H be a normal subloop of a loop G. Then every subloop S of the quotient loop G/H has a representation K/H where $K\geqq H$ is a unique subloop of G, namely the set of all elements of G contained in the cosets Hx belonging to S. Moreover K/H is a normal subloop of G/H if and only if K is a normal subloop of G; and when this is the case, G/K is isomorphic to $(G/H)/(K/H)$.*

Later we shall have occasion to refer to the Jordan-Hölder theorem and the Zassenhaus refinement theorem, which have been proved for arbitrary loops by Albert [2], Smiley [1], and Baer [3]. Albert has also shown that, for isotopic loops, normal subloops are isotopic in pairs, whence in particular the quotient loops in the composition series of isotopic loops are also isotopic in pairs.

In concluding this section we might remark that our inner mapping group $\mathfrak{J}$ has been put to quite a different use in earlier work. Baer has employed it in a representation of any loop as the set of cosets of a group $\mathfrak{G}$ modulo a non-normal subgroup $\mathfrak{J}$, under an unusual form of multiplication.

4. **π-series for loops.** We first define the notion of a *characteristic* property π. Let the statement "the element a of the loop G has property π with respect to G" (which, temporarily, we shall abbreviate to "$a\pi G$") be determinative. Then π will be called a characteristic property of loops if and only if it possesses the following properties[9] for every loop G:

[7] Baer [3, Theorem 1].

[8] See also Zassenhaus [1, p. 30].

[9] Our thanks are due to C. J. Everett for critical comments in this connection. We also take this opportunity to express our indebtedness to R. A. Good for many valuable improvements to Chapter I, and to §4 in particular.

(i) $1\pi G$, *where* 1 *is the unit of* G.

(ii) *If* $a\pi G$ *and* $a\in H$, *where* H *is a subloop of* G, *then* $a\pi H$ (distributivity to subloops).

(iii) *If* $a\pi G$ *and if* $GT=H$, $aT=b$, *where* T *is an isomorphic mapping of* G *upon* H, *then* $b\pi H$ (abstractness).

We note in passing that properties (i), (ii), (iii) may easily be shown to be independent—by consideration, for example, of the following properties π: "a is not the unit element of G"; "$a=x^2$ for some x of G"; "a is a matrix." The term *characteristic* is partly justified by the fact that the non-empty subset G_π of G, consisting of all a for which $a\pi G$, is mapped into itself by every automorphism of G, as follows from (iii). As an example of such a characteristic property we may cite the case "$a\in B$" where B is any fixed one of the characteristic subloops A_λ, A_μ, A_ρ, A or C dealt with in the preceding sections. Other examples will be encountered in Chapter II.

We now proceed to lay down a series of postulates which determine a class of so-called *π-admissible* loops, for any characteristic property π. These will eventually be employed (in Chapters I and II) to develop many concrete analogues for loops of the notion of central series of a group (P. Hall [1]). The reader may find it helpful to keep in mind the case where G is a group and where "$a\pi G$" means "a is in the centre of G." It seems proper to add that, inasmuch as characteristic subloops of a loop need not be normal (Baer [3]), it is necessary here to be more elaborately cautious than in the theory of groups.

DEFINITION. If π is a characteristic property of loops, we shall say that a loop G is *π-admissible* if and only if the following postulates (I), (II), (III), (IV) and (V) are satisfied.

I. *The set* G_π, *consisting of all elements a which have property* π *relative to* G, *is a subloop of* G.

DEFINITION. We designate by $Z\equiv Z_\pi(G)$ the union of all normal subloops of G which are contained in G_π. Z will be called the *π-centre*[10] of G.

Note that Z exists, by Theorem 3G. In fact Z is a subloop of G_π. More precisely, G_π and Z are respectively a characteristic subloop and a characteristic normal subloop of G.

II. *If* K *is a normal subloop of* G, *then* G/K *satisfies* (I).

III. *If* N *is any fixed normal subloop of* G, *there exists a non-empty subset* $S(N)\equiv S_\pi(N, G)$ *of* N *such that, for a normal subloop* K *of* G, $(NK)/K$ *is in* $Z_\pi(G/K)$ *if and only if* $K\geqq S(N)$.

Remark. We use $NK=\{N, K\}$ instead of N in order to cover the case that K is not a subloop of N.

DEFINITION. We designate by $H\equiv H_\pi(N, G)$ the intersection of all normal subloops of G which contain $S(N)$. Note that H is unique, even though $S(N)$ may not be.

[10] A more consistent term would be *π-or*, but this is unpalatable.

By Theorem 3E, H is a normal subloop of G; and clearly $H \leqq N$. In fact H is the smallest subloop of N, normal in G, such that $N/H \leqq Z_\pi(G/H)$.

IV. *If M, N are normal subloops of G then $M \leqq N$ implies $S(M) \leqq S(N)$.*

V. *Every subloop of G satisfies* (I), (II), (III) *and* (IV).

In the case that π is the property of lying in the centre the reader may find it of interest to verify that every associative loop G is π-admissible. (In fact $Z_\pi(G)$ and $H_\pi(N, G)$ are respectively the centre and the commutator subgroup (N, G).) And indeed, with this choice of π every loop is π-admissible; we leave the proof for a later section.

The following lemmas embody a number of simple facts about π-admissible loops.

Lemma 4A. *Let π be a characteristic property, G a π-admissible loop, and F a subloop of G. Then:*

(a) *F is π-admissible;*

(b) *$F \cap G_\pi \leqq F_\pi$;*

(c) *if $G_\pi \leqq F$ then $G_\pi \leqq F_\pi$;*

(d) *$F \cap Z_\pi(G) \leqq Z_\pi(F)$;*

(e) *if $Z_\pi(G) \leqq F$, then $Z_\pi(G) \leqq Z_\pi(F)$;*

(f) *if $F = Z_\pi(G)$ then $Z_\pi(F) = F$.*

Proof. (a) Clearly postulate (V) is the only one in question. If E is any subloop of F, E is a subloop of G and hence, by (V), E satisfies the first four postulates. Thus F satisfies (V).

(b) Since $F \cap G_\pi \leqq F$, the result follows by (ii) (distributivity to subloops).

(c) Since $G_\pi \leqq F$, $G_\pi = F \cap G_\pi \leqq F_\pi$, by (b).

(d) By Theorem 3H, $F \cap Z_\pi(G)$ is a normal subloop of F. But $Z_\pi(G) \leqq G_\pi$, and hence $F \cap Z_\pi(G) \leqq F \cap G_\pi \leqq F_\pi$, by (a). Thus $F \cap Z_\pi(G) \leqq Z_\pi(F)$.

(e) Since $Z_\pi(G) \leqq F$, $Z_\pi(G) = F \cap Z_\pi(G) \leqq Z_\pi(F)$, by (d).

(f) If $F = Z_\pi(G)$ then, by (e), $F = Z_\pi(G) \leqq Z_\pi(F) \leqq F$, whence $F = Z_\pi(F)$.

Lemma 4B. *If K, N are normal subloops of a π-admissible loop G, and if $K \leqq N$, then $H_\pi(K, G) \leqq H_\pi(N, G)$.*

Proof. By (IV) and the definition, $S(K) \leqq S(N) \leqq H_\pi(N, G)$. Hence $H_\pi(K, G)$, being the intersection of all normal subloops of G which contain $S(K)$, is a subloop of the normal subloop $H_\pi(N, G)$.

Lemma 4C. *If K is a normal subloop of a π-admissible loop G, then $H(K, G) = 1$ if and only if $K \leqq Z_\pi(G)$.*

Corollary 1. $H_\pi(1, G) = 1$.

Corollary 2. $H_\pi(Z_\pi(G), G) = 1$.

Proof. (Here 1 designates the subloop consisting of the unit element 1.) By its definition, $L = H_\pi(K, G)$ is the smallest subloop of K, normal in G, such that $K/L \leqq Z_\pi(G/L)$. Thus $L=1$ if and only if $K \leqq Z_\pi(G)$. The corollaries follow immediately.

Definition. A π-admissible loop G will be called a *π-loop* if and only if $G_\pi = G$; in other words, if and only if G coincides with its π-centre. As follows from Lemma 4A, part (f), every π-centre is a π-loop.

Definition. Let G be a π-admissible loop, and let (K), or

$$1 = K_0 \leqq K_1 \leqq \cdots \leqq K_m = G, \tag{4.1}$$

be an ascending chain of normal subloops of G, where m is a finite integer, called the *length* of (K). Such a chain (K) we shall call a ***proper π-series*** of G if and only if

$$H_\pi(K_i, G) \leqq K_{i+1}, \qquad i = 0, 1, \cdots, m-1. \tag{4.2}$$

We now define by recursion the series (H) or

$$H_1 = G, \qquad H_{i+1} = H_\pi(H_i, G), \qquad i = 1, 2, \cdots, \tag{4.3}$$

which is meaningful for any π-admissible loop.

Lemma 4D. *If the loop G is π-admissible, $H_i \geqq H_{i+1}$ for every positive integer i. And if there exists an integer i such that $H_{i+1} = H_i$ then $H_j = H_i$ for all $j \geqq i$.*

Proof. The first statement follows from the fact that $H_\pi(N, G) \leqq N$ for every normal subloop N of G. Again, if $H_j = H_i$ then $H_{j+1} = H_\pi(H_j, G) = H_\pi(H_i, G) = H_{i+1} = H_i$; hence the second statement may be proved by induction.

We shall refer to the series (H) as the *lower π-series* of G. If $H_i = H_{i+1}$ for a finite integer i we shall call H_i the *π-potent* of G. (The term is due to R. Baer.) If in addition $H_i = 1$, (H) is clearly a proper π-series when written in the order of decreasing indices.

Similarly for every π-admissible loop G we define the *upper π-series* (Z) by

$$Z_0 = 1, \qquad Z_i/Z_{i-1} = Z_\pi(G/Z_{i-1}), \qquad i = 1, 2, \cdots, \tag{4.4}$$

where it is understood for all $i \geqq 1$ that Z_i is the unique normal subloop of G referred to in Theorem 3K. Note that $Z_1 = Z_\pi(G) = Z$.

Lemma 4E. *If G is π-admissible, $Z_i \geqq Z_{i-1}$ for $i = 1, 2, \cdots$, and moreover $H_\pi(Z_i, G) \leqq Z_{i-1}$. If there exists a finite integer $i \geqq 1$ such that $Z_i = Z_{i-1}$, then $Z_j = Z_{i-1}$ for all $j \geqq i-1$.*

Proof. This is obvious.

If $Z_{i+1} = Z_i$ for some finite i, we shall call Z_i the *hyper-π-loop* of G. If in addition $Z_i = G$, (Z) is clearly a proper π-series.

Theorem 4A. *Let the π-admissible loop G possess a proper π-series (K) of* *length m, as given by* (4.1), (4.2). *Then*: (i) *the lower π-series* (H) *is a proper π-series of length l, where $l \leqq m$*; (ii) *the upper π-series* (Z) *is a proper π-series of length u, where $u \leqq m$*; (iii) $l=u$.

Definition. Under the hypothesis of Theorem 4A, the loop G will be called *π-nilpotent* of *class c*, where $c=c_\pi(G)$ is the common length $c=l=u$ of the upper and lower π-series.

Proof of Theorem 4A. (i) $H_1=K_m=G$, by definition, and so $H_1 \leqq K_m$. Assume inductively that $H_i \leqq K_{m+1-i}$ for some $i \geqq 1$. Then $H_{i+1} \equiv H_\pi(H_i, G) \leqq H_\pi(K_{m+1-i}, G) \leqq K_{m-i}$. Here we have used Lemma 4B and have tacitly assumed $i \leqq m$. Our induction is thus complete and yields in particular $H_{m+1} \leqq K_0=1$, whence $H_{m+1}=1$. If $l \geqq 0$ is the smallest integer for which $H_{l+1}=1$ we have $l \leqq m$. Moreover the series $1=H_{l+1}<H_l< \cdots <H_1=G$ is a proper π-series of length l in the sense of the original definition.

(ii) $K_0=Z_0=1$ and so $K_0 \leqq Z_0$. Assume inductively that $K_i \leqq Z_i$ for some $i \geqq 0$. Thus, by (4.2), $H_\pi(K_{i+1}, G) \leqq K_i \leqq Z_i$, and hence, by postulate (III), $(K_{i+1}Z_i)/Z_i$ is in $Z_\pi(G/Z_i)$, whence $K_{i+1}Z_i$ is in Z_{i+1} and $K_{i+1} \leqq Z_{i+1}$. (We have tacitly assumed $i+1 \leqq m$.) Thus our induction is complete, and in particular $G=K_m \leqq Z_m$. If u is the smallest integer such that $Z_u=G$ it follows that $u \leqq m$, and that (Z) is a proper π-series of length u.

(iii) Since (Z) is a proper π-series of length u, it follows from (i) that $l \leqq u$. Similarly (H) is a proper π-series of length l, and $u \leqq l$ by (ii). Thus $l=u$.

This is precisely analogous to the type of proof used by Hall [1].

Theorem 4B. *Let G be a π-nilpotent loop of class c. Then every subloop K of G is π-nilpotent of class not greater than c. More precisely, if $d \leqq c$ is the smallest integer for which $Z_d \geqq K$, then K has class not greater than d.*

Corollary. *If, under the above hypothesis, K is a simple loop not equal to* 1, *then K is a π-loop of class* 1, *and either $K \leqq Z$ or $K \cap Z=1$.*

Proof. We define the set (A) of subloops A_i by

$$A_i = K \cap Z_i, \qquad i = 0, 1, 2, \cdots, d. \tag{4.5}$$

Then from the definition of the Z_i we have $1=A_0 \leqq A_1 \leqq \cdots \leqq A_d=K$. Furthermore A_{i-1} is a normal subloop of K and of A_i (Theorem 3H and corollary). We now make two simultaneous applications of Theorem 3I, noting that $A_i \cap Z_{i-1}=K \cap Z_{i-1}=A_{i-1}$. Under the same isomorphism, A_i/A_{i-1} and K/A_{i-1} are respectively isomorphic to $(A_iZ_{i-1})/Z_{i-1}$ and $(KZ_{i-1})/Z_{i-1}$. But $A_iZ_{i-1} \leqq KZ_{i-1}$ and $A_iZ_{i-1} \leqq Z_i$, whence $A_iZ_{i-1} \leqq Z_i \cap (KZ_{i-1})$. By property (ii) of the characteristic property π, $(A_iZ_{i-1})/Z_{i-1}$ is in the π-centre of $(KZ_{i-1})/Z_{i-1}$; and the property (iii) of π, namely that such relations are preserved under isomorphism, insures that A_i/A_{i-1} is in the π-centre of K/A_{i-1}. That is, $A_i/A_{i-1} \leqq Z_\pi(K/A_{i-1})$; or equivalently, $H_\pi(A_i, K) \leqq A_{i-1}$. Therefore the series (A) is a proper π-series of K; and by Theorem 4A, K has class not greater than d.

The loop 1 is clearly π-nilpotent of class 0. If $K \neq 1$ is nilpotent but simple, so that K can have no proper normal subloops, it follows that $1 = Z_0(K) < Z_1(K) = K$, so that K has class 1, and K is a π-loop. Again, the subloop $A_1 = K \cap Z$, given by (4.5), where $Z = Z_1 = Z_\pi(G)$, is either 1 or K. This completes the proof of the corollary.

Lemma 4F. *Let G be a π-admissible loop, K a normal subloop of G. Then G/K is π-admissible.*

Proof. By postulate (II), (I) holds. Again, any normal subloop of G/K has a representation of form N/K where N is a uniquely defined normal subloop of G (Theorem 3K). By the same theorem $(G/K)/(N/K)$ is isomorphic to G/N; but (I) is satisfied in G/N, and hence (II) is satisfied in G/K. As to (III), we clearly may define $S(N/K, G/K) = S(N, G)/K$ and, with this definition, (IV) will be automatically verified. Finally (V) follows from the fact that every subloop of G/K has the form F/K where F is a subloop of G. Note incidentally that $H_\pi(N/K, G/K) = [H_\pi(N, G) \cdot K]/K$.

Theorem 4C. *Let K be a normal subloop of a π-nilpotent loop G, of class c. Then G/K is π-nilpotent of class not greater than $c-n$, where n is the largest integer such that $Z_n \leqq K$.*

Proof. Define a series (M) by

$$K = M_0, \qquad M_i/M_{i-1} = Z_\pi(G/M_{i-1}), \qquad i = 1, 2, \cdots. \tag{4.6}$$

Then clearly the series $(M_0/K) \leqq (M_1/K) \leqq \cdots$ will be the upper π-series of G/K. By assumption $Z_n \leqq M_0$. If for some $i \geqq 0$ we have $Z_{n+i} \leqq M_i$ then $H_\pi(Z_{n+i+1}, G) \leqq Z_{n+i} \leqq M_i$ and so, by the argument used in the proof of Theorem 4A, $Z_{n+i+1} \leqq M_{i+1}$. Thus $Z_{n+i} \leqq M_i$ for $i = 0, 1, \cdots$, and in particular $M_{c-n} = G$.

Corollary to Theorem 4C. *Under the hypothesis of Theorem 4C, K is contained in a π-series of G. In particular every minimal normal subloop of G is contained in the π-centre.*

In fact if m is the class of G/K we may choose $K_1, K_2, \cdots, K_m = K$ so that $K_1/K \geqq \cdots \geqq K_m/K$ is the lower π-series of G/K, and then define K_i for $i \geqq m+1$ by $K_i = H_\pi(K_{i-1}, G)$. If the H_i are defined as before by (4.3) we may prove inductively that $K_{m+i} \leqq H_i$ for $i \geqq 1$. Thus the series (K) ends in 1; it is clearly a π-series. If in particular K is a minimal normal subloop of G we must have $K_{m+1} = H_\pi(K, G) = 1$, whence, by Lemma 4C, K is in the π-centre $Z_\pi(G)$.

Definition. If G is a π-admissible loop we shall call $H_\pi(G, G) = G_\pi'$ the *π-derived* loop of G.

Definition. If the series (G^i), defined by

$$(4.7) \qquad G^0 = G, \qquad G^{i+1} = H(G^i, G^i), \qquad i = 0, 1, 2, \cdots,$$

ends in the identity we shall say that the π-admissible loop G is *π-solvable.* (Note that G^{i+1} is the π-derived loop of G^i.)

In Chapter III we shall exhibit an example to show that although G^{i+1} is normal in G^i, there exist π-admissible loops for which G^2 is not normal in G. Thus, in contrast with the usual situation in group theory, the series (G^i) is not necessarily a π-series.

If G is a finite π-admissible loop it may readily be deduced from the results of this section that G is π-solvable if and only if the simple factor-loops in its composition series are all π-loops. From this observation we obtain the analogue for π-admissible loops of a theorem on finite groups due to Fitting [1, Satz 1]:

Theorem 4D. *Every finite π-admissible loop G possesses one and only one maximal, π-solvable, normal subloop S, which contains every other π-solvable normal subloop of G. S is thus a characteristic subloop of G.*

Proof. By Theorem 3I, if H, K are normal subloops of G, $(HK)/H$ is isomorphic to $K/(H\cap K)$. Thus the simple factor-loops of HK, which, by the Jordan-Hölder Theorem, are uniquely defined in the sense of isomorphism, consist of the simple factor-loops of $K/(H\cap K)$ and of those of H. If H and K are π-solvable, all of these factor-loops are π-loops and hence the normal subloop HK is π-solvable. Similarly the union of any finite number of normal π-solvable subloops of G is a normal π-solvable subloop of G. Thus we may take S to be the union of all normal π-solvable subloops of G. Since π is a characteristic property, SA will be a normal π-solvable loop of G for every automorphism A of G. It follows that $SA \leqq S$, whence S is a characteristic subloop of G.

5. **The ϕ-loop of a loop.** Let x be an element of the arbitrary loop G. We shall call x a *non-generator* of G (B. Neumann [1]) if and only if $\{x, S\} = G$ implies $\{S\} = G$ for every subset S of G. The corresponding notion for groups is essentially due to G. Frattini [1].

Theorem 5A. *The set F of all non-generating elements of a loop $G \neq 1$ is a characteristic subloop of G. Moreover F is the intersection of all maximum subloops of G.*

Definition. F will be called the *ϕ-loop* of G, and will be designated by $\phi(G)$.

Proof. If a, b are non-generators, $\{ab, S\} = G$ implies $G = \{a, b, S\} = \{b, S\} = \{S\}$, since $\{a, b, S\}$ certainly contains $\{ab, S\}$. Similarly $\{aR_b^{-1}, S\} = G$ and $\{aL_b^{-1}, S\} = G$ separately imply $\{S\} = G$. Thus ab, aL_b^{-1} and aR_b^{-1} are non-generators, whence F is a subloop of G. If T is any automorphism of G, and S any subset of G, $\{S\}=G$ implies $\{ST\}=GT=G$; and from this fact it may be deduced that F is characteristic. We omit the proof of the second statement. The corresponding proof by B. Neumann [1], given for arbitrary groups, is valid without change for loops. (It should be noted that Neumann's proof is based on the axiom of choice.)

For the loop 1 of order one, where the notion of a non-generator is not very meaningful, we shall define the ϕ-loop to be the loop itself. For a loop $G\neq 1$, $\phi(G)$ cannot contain every element of G (as is trivially evident), and hence the series

$$G=F_0>F_1>F_2>\cdots, \tag{5.1}$$

where $F_i=\phi(F_{i-1})$ for $i=1, 2, \cdots$, is a strictly decreasing series of characteristic subloops of G. Moreover if G is a finite loop we must have $F_i=1$ for some i. The author has given several constructions (Bruck [3]) of simple finite loops G for which $\phi(G)$ is at the same time an arbitrary finite loop and a unique maximum subloop of G. By a repetition of such constructions the series (5.1) can be made to have any finite length, with none of the F_i a proper normal subloop of G. The contrast with the theory of ϕ-groups of a group is thus very marked (Miller [1, pp. 71–72]), unless attention is restricted to special classes of loops.

6. **Lagrange properties for finite loops.** The following property (L), when stated for finite groups, is known as Lagrange's Theorem:

(L) *The order of every subloop H of the finite loop G divides the order of G.*

Since every finite group G has property (L), the stronger property (L′) holds for groups:

(L′) *If K is any subloop of any subloop H of the finite loop G, the order of K divides the order of H.* More briefly, *every subloop of G has property* (L).

By use of one of the constructions in Bruck [3] one may obtain a loop F of order 5 with a subloop of order 2 but no other proper subloops. Thus F does not have property (L). Further one may construct a loop G of order 10, containing F as a unique maximum subloop (which is in fact normal in G). It follows that G has two subloops of orders 2 and 5, but no other proper subloops. Therefore G has property (L) but not, however, property (L′). On the other hand it should be obvious that *if a finite loop G has property* (L′) *then so does every subloop of G.*

Hausmann and Ore [1] have restricted their attention to quasigroups in which a coset expansion (in a sense wholly analogous to that for groups) exists with respect to every subquasigroup. Thus in their work property (L) and often property (L′) are trivially satisfied for finite quasigroups. The following treatment, to which we shall wish to refer in later sections, is wholly independent of the restrictive hypotheses of Hausmann-Ore.

THEOREM 6A. *Let G be a finite loop, and let the decreasing series of subloops*

$$G = C_0 \geqq C_1 \geqq \cdots \geqq C_r \geqq C_{r+1} = 1 \tag{6.1}$$

be such that C_{i+1} is a normal subloop of C_i and that C_i/C_{i+1} has property (L) *for $i=0, 1, 2, \cdots, r$. Then G has property* (L).

Proof. By hypothesis $C_r \equiv C_r/C_{r-1}$ has property (L). Assume inductively that C_i has property (L) for some i with $0 < i \leqq r$, and let S be any subloop of C_{i-1}. Then, since C_i is normal in C_{i-1}, $\{S, C_i\} = SC_i$ and $(SC_i)/C_i$ is isomorphic to $S/(S \cap C_i)$, as follows from Theorem 3I. Since $(SC_i)/C_i$ is a subloop of C_{i-1}/C_i, and since the latter has property (L), it follows that the order of $S/(S \cap C_i)$ divides the order of C_{i-1}/C_i:

$$[S:(S \cap C_i)] \mid [C_{i-1}:C_i], \tag{6.2}$$

where as usual $[A:B]$ refers to the order of A divided by the order of B, and $m \mid n$ means that the integer m divides the integer n. But also $S \cap C_i$ is a subloop of C_i and so, by our inductive hypothesis, we have

$$[(S \cap C_i):1] \mid [C_i:1]. \tag{6.3}$$

Since $[S:(S \cap C_i)] \cdot [(S \cap C_i):1] = [S:1]$ and $[C_{i-1}:C_i] \cdot [C_i:1] = [C_{i-1}:1]$ we see from (6.2) and (6.3) by multiplication that

$$[S:1] \mid [C_{i-1}:1]. \tag{6.4}$$

Thus C_{i-1} has property (L), whence Theorem 6A follows by induction.

Theorem 6B. *Let the finite loop G have a descending series* (6.1) *such that C_{i+1} is a normal subloop of C_i and C_i/C_{i+1} has property* (L′) *for $i=0, 1, 2, \cdots, r$. Then G has property* (L′). *Conversely, if G has property* (L′) *and if* (6.1) *is any descending series such that C_{i+1} is a normal subloop of C_i for $i=0, 1, 2, \cdots, r$, then C_i/C_{i+1} has property* (L′) *for $i=0, 1, 2, \cdots, r$.*

Proof. (a) *Sufficiency.* Assume that (6.1) is given with the prescribed properties and let H be any subloop of G. Since $C_0 \geqq H$ there exists a greatest integer $s \geqq 0$ such that $C_s \geqq H$, and we define

$$A_i = C_i \cap H, \qquad i = s, s+1, \cdots, r+1. \tag{6.5}$$

By Theorem 3J, A_{i+1} is a normal subloop of A_i for $i=s, s+1, \cdots, r$. Since $C_{i+1} \leqq C_i$ and $A_i \leqq C_i$ it follows that $A_iC_{i+1} \equiv \{A_i, C_{i+1}\} \leqq C_i$, whence $(A_iC_{i+1})/C_{i+1}$ is a subloop of C_i/C_{i+1} and thus has property (L′). Again, $A_i \cap C_{i+1} = H \cap C_i \cap C_{i+1} = H \cap C_{i+1} = A_{i+1}$; and so, since the loops $(A_iC_{i+1})/C_{i+1}$ and $A_i/(A_i \cap C_{i+1}) \equiv A_i/A_{i+1}$ are isomorphic, it follows that A_i/A_{i+1} has property (L′) for $i=s, s+1, \cdots, r$. An application of Theorem 6A now shows that $H = A_s$ has property (L), whence G has property (L′).

(b) *Necessity.* If G is a finite loop with property (L′) and if H is a normal subloop of G, it is a trivial consequence of the familiar Theorem 3K that G/H has property (L′). Now let (6.1) be any decreasing series of subloops of G with C_{i+1} normal in C_i for $i=0, 1, 2, \cdots, r$. Then since C_i, as a subloop of G, has property (L′), it results from the preceding remark that C_i/C_{i+1} has property (L′).

It should perhaps be noted that the trivial series $G \geqq 1$ has not been excluded as a series (6.1).

As may readily be deduced from Theorem 6B, *a necessary and sufficient condition that a finite loop G have property* (L′) *is that each of the simple factor-loops in a composition series of G have property* (L′). Albert [2, p. 412] defines a finite loop to be solvable provided each of its simple factor-loops is without proper subloops. Since a loop without proper subloops trivially has property (L′) we see that *every finite loop which is solvable in the sense of Albert has property* (L′).

The following theorem, which can in fact be deduced from Theorem 6A and the definitions of §4, has especial interest for the sequel.

THEOREM 6C. *The following properties are equivalent for any fixed characteristic property π:*

(i) *Every finite π-loop has property* (L′).

(ii) *Every finite π-nilpotent loop has property* (L′).

(iii) *Every finite π-solvable loop has property* (L′).

Proof. This is a simple corollary of Theorem 6B.

COROLLARY. *If the characteristic property π is so chosen that π-loops are groups then every finite π-solvable loop* (*and hence every finite π-nilpotent loop*) *has property* (L′).

The proof of the following theorem closely parallels that of Theorem 4D, and hence is omitted.

THEOREM 6D. *Every finite loop G contains one and only one maximal normal subloop S with property* (L′). *S contains every other normal subloop of G which has property* (L′), *and is thus a characteristic subloop of G.*

7. **Central series.** In this section the characteristic property π of §4 is taken to be that of belonging to the centre. Thus the element a of the loop G has property π with respect to G if and only if

$$(7\ 1) \qquad ax = xa, \qquad ax\cdot y = a\cdot xy, \qquad xa\cdot y = x\cdot ay, \qquad xy\cdot a = x\cdot ya$$

for all x, y of G. Then, for any loop G whatsoever, postulate (I) is satisfied; in fact $G_\pi = Z_\pi = Z$ is the centre of G. Moreover (II) is trivially satisfied. Before considering the remaining postulates it will be convenient to prove several lemmas.

LEMMA 7A. *Let H be a subloop of a loop G, and let $\mathfrak{M}$ be any set of mappings of H into itself. Let $H(\mathfrak{M})$ be the subloop of H generated by the set of all elements*

hUL_h^{-1} with h in H, U in $\mathfrak{M}$. Then if K is any subloop of G such that $H(\mathfrak{M}) \leqq K \leqq H$, K is mapped into itself by $\mathfrak{M}$.

Corollary. *$H(\mathfrak{M})$ is mapped into itself by $\mathfrak{M}$.*

Proof. Let x be any element of $K \leqq H$, U any element of $\mathfrak{M}$. Then the element $xUL_x^{-1} = y$ is in $H(\mathfrak{M}) \leqq K$ by hypothesis. Hence $xU = yL_x = xy$ is in K.

Lemma 7B. *Let N be a normal subloop of a loop G, and let $\mathfrak{J}$ be the inner mapping group of G. Then $N(\mathfrak{J})$, the subloop of N generated by the set of all elements nUL_n^{-1} with n in N, U in $\mathfrak{J}$, is a normal subloop of G.*

Proof. This follows from Lemma 7A and the fact that a subloop of G is normal in G if (and only if) it is mapped into itself by $\mathfrak{J}$.

Definition. If N is a normal subloop of a loop G we designate by (N, G) the normal subloop $N(\mathfrak{J})$ defined in Lemma 7B.

Lemma 7C. *Let $\mathfrak{J}$ be the inner mapping group of a loop G, and let $\mathfrak{M}$ be any set of generators of $\mathfrak{J}$. Then if N is a normal subloop of G, (N, G) is generated by the set of all elements nUL_n^{-1} with n in N, U in $\mathfrak{M}$.*

Proof. Let the elements nUL_n^{-1} generate the loop K. Since N is a normal subloop of G, N is certainly mapped into itself by $\mathfrak{M}$. Thus, by Lemma 7A, K is mapped into itself by $\mathfrak{M}$. Since $\mathfrak{M}$ generates $\mathfrak{J}$, K is also mapped into itself by $\mathfrak{J}$, and hence is a normal subloop of G. Where U, V are in $\mathfrak{J}$, suppose that it has already been shown that nUL_n^{-1} and nVL_n^{-1} are in K for all n of N. Thus $nUL_n^{-1} = k \in K$; or $nU = nk$. Hence $n = (nk)U^{-1} = kP \cdot nU^{-1}$ for $P \in \mathfrak{J}$, whence $n \in K(nU^{-1}) = (nU^{-1})K$, or $nU^{-1} \in nK$, $nU^{-1}L_n^{-1} \in K$. Again $n(UV) = (nU)V = (nk)V = kQ \cdot nV$ for $Q \in \mathfrak{J}$, whence $n(UV) \in K \cdot nK = nK$ or $n(UV)L_n^{-1} \in K$. Thus $nU^{-1}L_n^{-1}$ and $nUVL_n^{-1}$ are also in K, and it follows by mathematical induction that nUL_n^{-1} is in K for every U of $\mathfrak{J}$. Therefore, since K is a subloop, $(N, G) \leqq K$. But it is trivially evident that $K \leqq (N, G)$, and so $K = (N, G)$.

Lemma 7D. *Where N is a normal subloop of the loop G, let $S(N)$ be the set of all elements $nT_xL_n^{-1}$, $nR_{x,y}L_n^{-1}$, $nL_{x,y}L_n^{-1}$ with n in N, x, y in G, where*

$$T_x = R_xL_x^{-1}, \qquad R_{x,y} = R_xR_yR_{xy}^{-1}, \qquad L_{x,y} = L_xL_yL_{yx}^{-1}. \tag{7.2}$$

Then if K is a normal subloop of G, a necessary and sufficient condition that $(NK)/K$ be in the centre of G/K is that $K \geqq S(N)$.

Theorem 7A. *Let N, K be normal subloops of the loop G. Then a necessary and sufficient condition that $(NK)/K$ be in the centre of G/K is that $K \geqq (N, G)$.*

Corollary. *Where $S(N)$ has been defined in Lemma 7D, $\{S(N)\} = (N, G)$.*

Proof of Lemma 7D and Theorem 7A. Necessary and sufficient conditions that the coset nK be in the centre of G/K may be written as follows, where

x, y range over all elements of G:

$$(nx)K = (xn)K, \quad (nx\cdot y)K = (n\cdot xy)K, \quad (xn\cdot y)K = (x\cdot ny)K, \quad (xy\cdot n)K = (x\cdot yn)K. \tag{7.3}$$

By use of (7.2) the first relation of (7.3) may be written equivalently in any one of the following ways: $[x\cdot(nT_x)]\cdot K=(xn)K$; $(xK)[(nT_x)K]=xK\cdot nK$; $(nT_x)K=nK$; $nT_x\in nK$; $nT_xL_n^{-1}\in K$. Similarly the second and the fourth relations of (7.3) are respectively equivalent to $nR_{x,y}L_n^{-1}\in K$ and $nL_{y,x}L_n^{-1}\in K$. Hence the condition $K\geqq S(N)$ is necessary. The third relation of (7.3) may be written in the equivalent form

$$nC_{x,y}L_n^{-1} \in K, \qquad C_{x,y} = L_xR_yL_x^{-1}R_y^{-1}. \tag{7.4}$$

It was shown in §3 that the set of all permutations $R_{x,y}$ and $M_{x,y}$, where

$$M_{x,y} = R_yL_xR_{xy}^{-1} = T_yL_{y,x}T_{xy}^{-1}, \tag{7.5}$$

is a set of generators of $\mathfrak{J}$. Thus the set of all permutations $R_{x,y}$, $L_{x,y}$ and T_x also generates $\mathfrak{J}$, whence, by Lemma 7C, $\{S(N)\}=(N, G)$. Hence the condition $K\geqq(N, G)$ is also necessary.

Conversely, if $K\geqq S(N)$ then $K\geqq\{S(N)\}=(N, G)$. But $1C_{x,y}=(xy)L_x^{-1}R_y^{-1}=1$, so $C_{x,y}\in\mathfrak{J}$. Thus $nC_{x,y}L_n^{-1}$ is in (N, G) and hence in K. But it should be clear from what has gone before that the conditions $K\geqq S(N)$ and $K\ni nC_{x,y}L_n^{-1}$ for all $n\in N$, all $x, y\in G$, are together sufficient as well as necessary in order that $(NK)/K$ be in the centre of G/N. This completes the proof.

If we either take $S(N)$ as in Lemma 7D or set $S(N)=(N, G)$ there is no difficulty in verifying that the remaining postulates (III), (IV), and (V) are satisfied with $H_\pi(N, G)=(N, G)$. Hence all the results of §4 are valid in the present circumstances. We may either drop the prefix "π" or replace it by the adverb "centrally."

Every loop is centrally admissible. In a centrally nilpotent loop the upper and lower central series have the same length c, the central class of the loop (Theorem 4A). *Every subloop of a centrally nilpotent loop is centrally nilpotent* (Theorem 4B). *If K is a normal subloop of the centrally nilpotent loop G, then G/K is centrally nilpotent; moreover K is contained in a central series of G* (Theorem 4C and corollary). *The subloop* $(G, G)\equiv G'$ *we call the* (*centrally*) *derived loop of G.*

It follows from the general definition in §4 that a centrally solvable loop is one in which the series $G=G^0\geqq G^1\geqq G^2\geqq\cdots$, defined recursively by

$$G^0 = G, \qquad G^{i+1} = (G^i, G^i), \qquad i = 0, 1, 2, \cdots, \tag{7.6}$$

ends in the identity after a finite number of steps. It is to be noted that for any loop G, G/G' is a "central" loop, that is, an abelian group. Thus the successive quotients G^i/G^{i+1} are all abelian groups. Since every isotope of a group is an isomorphic group, and since isotopic loops have isotopic quotient loops, it follows that *every loop isotopic to a centrally solvable loop is centrally solvable.* To this extent the present definition of solvability is superior to that given by Albert. (See Albert [2] for his definition of solvability and for the theorems to which we have just appealed.) It may also be stated, on like grounds, that *every loop isotopic to a centrally nilpotent loop is centrally nilpotent.*

Finally we note that, since "central" loops are abelian groups, it follows from Theorem 6C that *the order of every subloop of a finite centrally nilpotent (or centrally solvable) loop divides the ordιr of the loop.* More specifically, *finite centrally nilpotent or solvable loops have property* (L′).

LEMMA 7E. *Let the loop G have centre $Z\neq 1$. Let H be a proper subloop of G with the properties $H\cap Z=1$, $HZ=G$. Then G is the direct product of H and Z: $G=H\times Z$.*

COROLLARY. $G'\leqq H$.

Proof. In what follows let h's and z's refer respectively to elements of H and of Z. By assumption, every element of G has a representation hz. But this representation is unique, for if $hz=h_1z_1$ then $h\cdot zz_1^{-1}=h_1$ or $h_1L_h^{-1}=zz_1^{-1}\in(H\cap Z)=1$, so $h_1=h$, $z_1=z$. Finally, the equation

$$h_1z_1\cdot h_2z_2 = h_3z_3 \tag{7.7}$$

is equivalent to the two equations

$$h_1h_2 = h_3, \qquad z_1z_2 = z_3. \tag{7.8}$$

It follows that $G=H\times Z$ (Albert [2]) and, as a consequence, that H is a normal subloop of G. (This might also be verified by use of one of the criteria discussed in §3.) Thus G/H is isomorphic to the abelian group Z, whence $H\geqq(G, G)=G'$. (It may indeed be shown by direct computation with $\mathfrak{J}$ that $H'=G'$, but we shall not use this fact.)

THEOREM 7B. *Let $G\neq 1$ be a finite centrally nilpotent loop, H a maximum subloop of G. Then* (i) $H\geqq G'$; (ii) *H is a normal subloop of G*; (iii) *H has prime index in G.*

Proof. First we note that (ii) and (iii) are immediate consequences of (i). In fact if H/G' is a maximum subgroup of the abelian group G/G' then H/G' is normal in G/G' and the group $(G/G')/(H/G')$ or G/H is a cyclic group of prime order.

As to (i), it is certainly true when G has prime order p, since in this case G is a cyclic group. Thus we may assume inductively that (i) is true for any finite centrally nilpotent loop L such that the total number of prime factors in the order of L (counted with their multiplicities) is less than the corresponding number for G. Since $G \neq 1$ we have $Z \neq 1$ by hypothesis. If we define Z_1 by

$$Z_1 = H \cap Z \tag{7.9}$$

the case $Z_1 = 1$ may be disposed of immediately. In fact, $Z_1 = 1$ implies $H < HZ$, whence, since H is maximum, $HZ = G$ and we may appeal[11] to Lemma 7E. Again, if $Z_1 \neq 1$, then Z_1, as a subloop of the centre G, is a normal subloop of G (a proper normal subloop, since $1 < Z_1 \leqq H < G$) and our inductive hypothesis allows us to assume that (i) holds for the finite centrally nilpotent loop G/Z_1. (Cf. Theorem 4C.) Since H/Z_1 is a maximum subloop of G/Z_1 we have $H \geqq K$ where K/Z_1 is the derived loop of G/Z_1. But G/K is isomorphic to the abelian group $(G/Z_1)/(K/Z_1)$, and therefore $K \geqq G'$. Hence $H \geqq K \geqq G'$, and the proof is complete.

LEMMA 7F. *Let G be a finite centrally nilpotent loop, H a subloop of prime index in G. Then H is a maximum subloop of G.*

COROLLARY. *A subloop of a finite centrally nilpotent loop $G \neq 1$ is maximum in G if and only if it has prime index in G.*

Proof. Let a be any element of G which is not in H, and set $K = \{a, H\}$. Then $[K:H] \neq 1$ but $[G:H] = [G:K][K:H] = p$ where p is a prime. Thus $[G:K] = 1$, $G = K$, H is a maximum subloop of G. The corollary follows from Lemma 7F and Theorem 7B.

We note in passing that Theorem 7B and the corollary to Lemma 7F indicate a method by which we may obtain a rather weak analogue, for a finite centrally nilpotent loop G, of the notion of *normalizer*. Let H be a proper subloop of G. Then among the set of all subloops $\{a, H\}$ with a in G but not in H there must exist at least one subloop K such that H is maximum in K. Since K is a finite centrally nilpotent loop, H is a normal subloop of prime index in K. It follows that *we may define a strictly increasing series of subloops $H = H_0 < H_1 < \cdots$, which ends in G, such that H_i is a normal subloop of prime index in H_{i+1}* for $i = 0, 1, \cdots$. Clearly this result is analogous to the one which states that in a finite nilpotent group G one may reach the whole group G from any subgroup H by the process of taking successive normalizers. However it lacks the important property of uniqueness.

THEOREM 7C. *The ϕ-loop $D = \phi(G)$ of a finite centrally nilpotent loop G is a characteristic normal subloop of G, and G/D is an abelian group.*

Proof. By Theorem 5A, D is characteristic and is the intersection of all maximum subloops of G. Since, by Theorem 7B, maximum subloops are nor-

[11] Indeed we may even obtain a contradiction, on the ground that $H \neq 1$ is centrally nilpotent and that the centre of a direct product is the direct product of the centres. Thus every maximum subloop of a finite centrally nilpotent loop has a nontrivial intersection with the centre.

mal, D is normal. Finally since every maximum subloop contains G', $D \geqq G'$, and so G/D is an abelian group.

Definitions. *If G is a finite centrally nilpotent loop, let $\mathfrak{P}$ be the set of all primes p for which there exists a maximum subloop H of index p in G.*

For each fixed p in $\mathfrak{P}$ let D_p be the intersection of all maximum subloops of index p in G.

Theorem 7D. *If G is a finite centrally nilpotent loop, then for each p of $\mathfrak{P}$, D_p is a characteristic normal subloop of G, and G/D_p is an elementary abelian group of type $(p, p, \cdots)$. Moreover $D=\phi(G)$ is the intersection of all the D_p, and the abelian group G/D is isomorphic to the direct product of the groups G/D_p.*

Proof. Since D_p is the intersection of all maximum subloops of index p it is clearly characteristic; it is also normal by Theorem 7B. From the definition of the D_p it is evident that D is their intersection.

Let M be any maximum subloop of index p in G, let x be any element of G, and let x^p designate any "pth power" of x, the grouping of the factors being quite arbitrary. Then since G/M is a cyclic group of order p, $(xM)^p = x^pM \leqq M$, or $x^p \in M$. Since this is true for any such x and any such M, we have $x^p \in D_p$. Moreover since $M \geqq G'$ for each such M we have $D_p \geqq G'$. Thus G/D_p is an abelian group in which each element save the identity has order p; in other words, G/D_p is an elementary abelian group of type $(p, p, \cdots)$.

Now let N be the product of the distinct primes p contained in the set P, and write $N/p = N_p$. If x is any element of G, then, since G/D is an abelian group, the coset $x^N D$ is the same for every grouping of the factors in the "power" x^N. In particular $x^N D = (x^{N_p})^p \cdot D$ for each p of P. Now $(x^{N_p})^p$ and D are both in D_p, whence $x^N D$ is in D_p for each p of P, or $x^N D$ is in D. Thus *the order of every element of G/D is a divisor of N.* It follows at once from the theory of abelian groups that G/D is a direct product of groups Δ_p/D, $p \in \mathfrak{P}$, where Δ_p/D is the unique subgroup of G/D, consisting of all elements of G/D whose orders divide p. Thus Δ_p is a unique normal subloop of G.

If Δ_p' is defined to be the union of the Δ_q with $q \neq p$, then it is clear that Δ_p'/D is the direct product of the Δ_q/D with $q \neq p$ and that $G/D = (\Delta_p/D) \times (\Delta_p'/D)$. Thus G/Δ_p', or the isomorphic group $(G/D)/(\Delta_p'/D)$, is isomorphic to Δ_p/D. Since $\Delta_p' \geqq D$ and since G/Δ_p' is elementary abelian of type $(p, p, \cdots)$, it follows that $\Delta_p' \geqq D_p$. But also we must have $\Delta_p \geqq D_q$ for $q \neq p$, and hence $\Delta_p' = D_p$, inasmuch as $\Delta_p' \cap \Delta_p = D$. This completes the proof of Theorem 7D.

Definition. A set B of elements of a loop G will be said to constitute a *basis* of G if $\{B\} = G$, and a *minimal basis* of G if in addition $\{C\} < G$ for any proper subset C of B.

The following theorem reduces to the well known Burnside basis theorem in the special case mentioned in Corollary 2. In any case the proof is based on that of P. Hall [1, Theorem 1.2, p. 35].

THEOREM 7E. *Let G be a finite centrally nilpotent loop and let x_1D, x_2D, $\cdots$, x_rD form a minimal basis of G/D, where $D=\phi(G)$. Then $x_1, x_2, \cdots, x_r$ form a minimal basis of G. Conversely, if $y_1, y_2, \cdots, y_s$ is any basis of G, the set of cosets $y_1D, y_2D, \cdots, y_sD$ contains a minimal basis of G.*

COROLLARY 1. *A necessary and sufficient condition that every minimal basis of G contain exactly n elements is that this be true for the abelian group G/D.*

COROLLARY 2. *If G/D is a p-group of order p^d, every minimal basis of G contains exactly d elements.*

Proof. Assume if possible $\{x_1, x_2, \cdots, x_r\} \equiv H \neq G$. Then H is contained in a maximum subloop M of G. But since $M \geqq D$ we have that M/D contains the set of cosets $x_1D, x_2D, \cdots, x_rD$, in contradiction to the hypothesis that the latter generate G/D. Conversely if $\{y_1, y_2, \cdots, y_s\}=G$ then $y_1D, y_2D, \cdots, y_sD$ generate G/D. Hence the set of cosets y_iD is either a minimal basis of G/D or contains a minimal basis as a proper subset.

Corollary 1 is a trivial consequence of Theorem 7E, and Corollary 2 follows from Corollary 1 and the well known fact that every minimal basis of an elementary abelian group of order p^d contains exactly d elements.

In connection with Corollary 1 it seems worthwhile to mention the following readily proved fact. Let the abelian group A be the direct product of n cyclic groups A_i where A_i has prime order p_i and the p_i are all distinct. Then A has a minimal basis consisting of one element; and indeed it has a minimal basis consisting of r elements for every integer r in the interval $1 \leqq r \leqq n$.

In the two theorems which follow we shall assume that G is a finite centrally nilpotent loop, that the centrally derived loop G' and the ϕ-loop $D=\phi(G)$ have orders u and v respectively, and that G/D has order $p(1)^{d(1)}p(2)^{d(2)} \cdots p(r)^{d(r)}$ where the $p(i)$ are distinct primes, the $d(i)$ positive integers. According to Theorem 7D, the abelian group G/D is a direct product of r elementary abelian p-groups E_i/D, where E_i/D has order $p(i)^{d(i)}$ and is in fact the uniquely defined subgroup of G/D consisting of all elements whose orders divide a power of $p(i)$. Each minimal basis of E_i/D consists of precisely $d(i)$ members.

Again we borrow from P. Hall [1]. For each fixed i, let us suppose that the ordered set

$$P(i, 1), P(i, 2), \cdots, P(i, d(i)) \tag{7.10}$$

is a set of representatives in E_i (and hence in G) of a minimal basis of E_i/D. We regard two such sets (7.10) as the same if and only if they consist of the same elements in the same order. If we denote the ordered set (7.10) by B_i, then the set B, consisting of all of the elements of the sets $B_1, B_2, \cdots, B_r$, will be termed a canonical basis of G. As in the proof of Theorem 7E we may show that a canonical basis is in fact a basis of G. Furthermore we regard two canonical bases B, C as the same if and only if, for each i, the ordered sets C_i, B_i are the same.

There are k_i ordered minimal bases $P(i, 1)D, \cdots, P(i, d(i))D$ of E_i/D, where

$$(7.11) \qquad k_i = (p(i)^{d(i)} - 1) \cdots (p(i)^{d(i)} - p(i)^{d(i)-1}).$$

Moreover each such basis is represented by $v^{d(i)}$ distinct ordered sets B_i. Thus, if in each group E_i/D a definite ordered minimal basis be chosen, we derive a total of v^d corresponding canonical bases B, where

$$(7.12) \qquad d = d(1) + d(2) + \cdots + d(r).$$

And finally we see that the total number of canonical bases is

$$(7.13) \qquad k = v^d k_1 k_2 \cdots k_r.$$

THEOREM 7F. *In the notation above, the order of the group $\mathfrak{A}$, consisting of all automorphisms of the finite centrally nilpotent loop G, is a divisor of k.*

Proof. Since the subloop E_i clearly is characteristic, every automorphism S of G maps the set of ordered sets B_i into itself, and hence S maps the set of all canonical bases into itself. Thus $\mathfrak{A}$ divides the set of canonical bases into b classes, each class containing all bases which can be derived from any fixed member of the class by the automorphisms of $\mathfrak{A}$. An automorphism S which leaves a given canonical basis B fixed, that is, which maps each element of B into itself, must be the identity automorphism. In fact $\{B\} = G$ and so we have $xS = x$ for every element x of G. It follows that $\mathfrak{A}$ permutes the elements of each class *regularly*. Thus if $\mathfrak{A}$ has order a, each class has a members. Hence the total number of classes is $ab = k$; and we see that a divides k.

It is natural to define the group of *inner automorphisms* of a loop G to be the intersection $\mathfrak{A} \cap \mathfrak{J}$ of $\mathfrak{A}$ and the inner mapping group of G. This definition leads to the following theorem.

THEOREM 7G. *With the hypotheses and notations of Theorem* 7F, *the order of the inner automorphism group of G is a divisor of v^d (and in fact of u^d).*

Proof. By multiplying the elements of a fixed canonical basis B of G by the elements of the centrally derived loop G' (of order u) we obtain u^d distinct sets C. Since $G' \leqq D$; each C is a canonical basis. If $S \in (\mathfrak{A} \cap \mathfrak{J})$, xSL_x^{-1} is in G' for every x of G; and thus, in particular, the aforementioned set of u^d bases is mapped into itself by $\mathfrak{A} \cap \mathfrak{J}$. As in the proof of Theorem 7F we deduce that the order of $\mathfrak{A} \cap \mathfrak{J}$ divides u^d (and hence also v^d).

In the special case that G is a finite p-group, Theorems 7F, 7G and their proofs are due to Hall [1].

8. **The inner mapping group of a centrally nilpotent loop.** If G is a group with centre Z and inner mapping group $\mathfrak{J}$ it is well known that $\mathfrak{J}$, which is in this case the group of inner automorphisms of G, is isomorphic to G/Z.

Thus the associated group $G=\{R_x, L_x; x\in G\}$ is simply the so-called holomorph of G, and a great deal is known about the relationships between G, $\mathfrak{J}$ and $\mathfrak{G}$. In the more general case that G is a loop, only a very few properties of $\mathfrak{J}$ and $\mathfrak{G}$ have been developed so far in this paper. They may be summed up as follows: $\mathfrak{J}$ consists of all elements U of G such that $1U=1$, where 1 is the unit element of G. Several sets of generators of $\mathfrak{J}$ have been given. A subloop H of G is normal in G if and only if $H\mathfrak{J}\leqq H$. Finally, if G is finite, $\mathfrak{G}:I=(G:1)\cdot(\mathfrak{J}:I)$, where I is the identity mapping of G; and $\mathfrak{G}:I$ divides $g!$ where $g=G:1$.

Certain questions come to mind at once, among which we shall mention the following.

(i) *In case the loop G is finite, what can be said about the order of $\mathfrak{J}$?*

(ii) *What can be stated about $\mathfrak{J}$ and $\mathfrak{G}$ when the loop G (finite or infinite) is centrally nilpotent?*

The situation in regard to (i) is in general quite complex. For example, it is easy to construct a non-associative loop of order 5 for which $\mathfrak{J}$ and $\mathfrak{G}$ have (Albert [2]) respectively the maximum possible orders 4! and 5!, while, at the other end of the scale, for an abelian group G, $\mathfrak{J}$ has order 1 and $\mathfrak{G}$ is isomorphic to G. In this section, however, we shall show that if G is a finite centrally nilpotent loop of order g then the orders of $\mathfrak{J}$ and $\mathfrak{G}$ divide some power of g. In connection with (ii) it will be convenient to introduce a definition.

Definition. A finite loop G will be said to be a finite p-loop if and only if p is a prime and the order of G is a power of p. Since there exist loops of prime order with nontrivial subloops one cannot hope for too much from a general study of p-loops, but the results already obtained in this paper should make it apparent that the class of finite centrally nilpotent p-loops will repay further study. At one stage in his research the author went so far as to produce a "proof" that a finite loop is centrally nilpotent if and only if it is a direct product of finite centrally nilpotent p-loops. This highly desirable result, true for groups, is unfortunately false for loops[12], and a counter example of order 6 will be given in Chapter III. It might be added that the decisive error was connected with (ii), which we shall study presently with greater care.

The following lemma is based upon an idea essentially due to Albert [1, 2], but used here in a slightly disguised form.

Lemma 8A. *Let G be a loop with inner mapping group $\mathfrak{J}$. Let H be a normal subloop of G, and let $\mathfrak{J}_H\leqq\mathfrak{J}$ be the set of all U in $\mathfrak{J}$ such that xU is in xH for every x of G. Then $\mathfrak{J}_H$ is a normal subgroup of $\mathfrak{J}$, and the inner mapping group $\mathfrak{J}(G/H)$ of G/H is isomorphic to $\mathfrak{J}/\mathfrak{J}_H$.*

Proof. We may set up a correspondence $U\rightarrow U'$ between the elements of

[12] We seize the present opportunity to apologize for an enthusiastic misstatement in this connection at a meeting of this Society, Chicago, November 1944.

$\mathfrak{I}=\mathfrak{I}(G)$ and those of $\mathfrak{I}(G/H)$ by use of the following definition:

$$(8.1) \qquad (xH)U' = (xU)H.$$

First we note that (8.1) defines U' unambiguously as a mapping of the cosets xH of G/H. In fact if $xH=yH$ then $y=xh$ for h in H, and so $yU=(xh)U=(xU)k$ for k in H, or $(yU)H=(xU)H$. Again, the set of all mappings $(R_{x,y})'$ and $(M_{x,y})'$ defined according to (8.1) is a subset and in fact a generating subset of $\mathfrak{I}(G/H)$, as may readily be verified. Moreover $(UV)'=U'V'$, and so the mapping $U\rightarrow U'$ is a homomorphism of $\mathfrak{I}$ upon $\mathfrak{I}(G/H)$. Thus $\mathfrak{I}(G/H)$ is isomorphic to $\mathfrak{I}/\mathfrak{K}$, where $\mathfrak{K}$ is the kernel of the homomorphism, namely the set of all U in $\mathfrak{I}$ such that $(xU)H=xH$ for all x in G. Since $(xU)H=xH$ if and only if xU is in xH we see that the normal subgroup $\mathfrak{K}$ is identical with $\mathfrak{I}_H$, and the proof is complete.

LEMMA 8B. *Let G be a loop with centre Z, and let G/Z have order r (finite or transfinite). Then the group $\mathfrak{I}_Z$ defined as in Lemma* 8A *is isomorphic to a subgroup of the rth direct power $P^r(Z)$ of Z. Thus in particular, $\mathfrak{I}_Z$ is an abelian normal subgroup of $\mathfrak{I}$.*

COROLLARY. *If G is a finite loop of order g. the order of $\mathfrak{I}_Z$ divides some (finite) power of g.*

Proof. By the rth direct power of Z we mean of course the direct product of r groups each isomorphic to Z. For convenience let us write $\mathfrak{K}=\mathfrak{I}_Z$. If U is in $\mathfrak{K}$ then to each element x of G there corresponds a centre element u such that $xU=xu$. But if $y=xz$ for z in Z then $yU=(xz)U=(xU)z=xu\cdot z=xz\cdot u=yu$. Hence to each element y of the coset xZ there corresponds the *same* centre element u such that $yU=yu$. It follows that U is completely and unambiguously determined by its effect on an arbitrarily selected element of each coset. Furthermore if V is also in $\mathfrak{K}$ and if $xV=xv$ then $x(UV)=(xu)V=xu\cdot v=x\cdot uv=x(VU)$; and of course, since $xU=xu$, $x=(xu)U^{-1}=(xU^{-1})u$ or $xU^{-1}=xu^{-1}$. Thus each fixed coset xZ sets up a uniquely determined homomorphism of $\mathfrak{K}$ into Z. It follows that these homomorphisms may be combined to yield a homomorphism θ of $\mathfrak{K}$ into $P^r(Z)$. But if the element U of $\mathfrak{K}$ corresponds under θ to the unit element of $P^r(Z)$ we have $xU=x$ for every x of G, or $U=I$. Thus, finally, $\mathfrak{K}$ is *isomorphic* with a subgroup of $P^r(Z)$. We have not assumed the finiteness of r, but the case of finite r is of special interest. As to the corollary, the order of Z divides g, and hence the order of $\mathfrak{K}$ divides g^r. In fact, since the homomorphism of $\mathfrak{K}$ set up by the identity coset Z is a homomorphism upon 1, the order of $\mathfrak{K}$ divides g^{r-1}. But the less precise result given in the corollary will be sufficient for our purposes.

We now combine the two preceding lemmas to derive the following:

THEOREM 8A. *Let G be a centrally nilpotent loop of (finite) class c, so that the upper central series of G is*

$$1 = Z_0 < Z_1 < \cdots < Z_c = G, \tag{8.2}$$

where Z_i/Z_{i-1} is the centre of G/Z_{i-1} for $i=1, 2, \cdots, c$. Then there exists an ascending series

$$I = \mathfrak{K}_0 < \mathfrak{K}_1 < \cdots < \mathfrak{K}_{c-1} = \mathfrak{K}_c = \mathfrak{I}, \tag{8.3}$$

of subgroups of the inner mapping group $\mathfrak{I}$, with the following properties, for $j=0, 1, 2, \cdots, c-1$:

(i) *$\mathfrak{K}_j$ is a normal subgroup of $\mathfrak{I}$;*

(ii) *the inner mapping group of G/Z_j is isomorphic to $\mathfrak{I}/\mathfrak{K}_j$;*

(iii) *$\mathfrak{K}_{j+1}/\mathfrak{K}_j$ is an abelian group isomorphic to a subgroup of $P^{r_j}(Z_{j+1}/Z_j)$, where r_j is the order of G/Z_j.*

COROLLARY I. *If the centrally nilpotent group G has finite order g then $\mathfrak{I}$ is a solvable group and the order of $\mathfrak{I}$ divides some finite power of g. (Hence, also, the order of the associated group $\mathfrak{G}$ divides some power of g.)*

COROLLARY II. *If G is a finite centrally nilpotent p-loop, both $\mathfrak{I}$ and $\mathfrak{G}$ are finite p-groups.*

Proof. Since centrally nilpotent loops of classes 0 or 1 are abelian the theorem is trivially verified for $c=0$ or 1. Hence we may make an induction on the class of G. Since $Z_1=Z$ is the centre of G we set $\mathfrak{K}_1=\mathfrak{I}_Z$, and it follows from Lemmas 8A, 8B that properties (i) and (ii) are satisfied for $j=0$, 1, and that (iii) is true for $j=0$. But G/Z_1 has class $c-1$, and so the rest of the theorem follows by mathematical induction.

In connection with the first statement of Corollary I it seems desirable to explain our use of the word "solvable," which is taken to be distinct from "nilpotent."

DEFINITION. *A finite group will be said to be solvable if and only if the factor groups in its decomposition series are all cyclic groups of prime order.*

With this definition the first statement is readily verified, and the second statement follows from (iii). (Compare the proof of the corollary of Lemma 8B.) Corollary II is a special case of Corollary I.

THEOREM 8B. *Let the loop G have upper central series (Z_i), so that $Z_0=1$ and Z_i/Z_{i-1} is the centre of G/Z_{i-1} for $i=1, 2, \cdots$. Let $\mathfrak{I}$ and $\mathfrak{G}$ be respectively the inner mapping group and the associated group of G, and let an ascending series $(\mathfrak{I}_i)$ of subgroups of G be defined as follows: $\mathfrak{I}_0=\mathfrak{I}$, and $\mathfrak{I}_i$ is the normalizer of $\mathfrak{I}_{i-1}$ in $\mathfrak{G}$ for $i=1, 2, \cdots$. Then $\mathfrak{I}_i$ is the set of all elements UR_x with U in $\mathfrak{I}$ and x in Z_i.*

COROLLARY I. *A necessary and sufficient condition that G be centrally nilpotent of (finite) class c is that $\mathfrak{I}_c=\mathfrak{G}$ but $\mathfrak{I}_{c-1}\neq\mathfrak{G}$.*

COROLLARY II. *If a finite loop G is centrally nilpotent the associated group $\mathfrak{G}$ is solvable.*

COROLLARY III. *A sufficient condition that a finite loop G be centrally nilpotent of class not greater than c is that the associated group $\mathfrak{G}$ be nilpotent of class c.*

Proof. Let us assume temporarily the truth of Theorem 8B and dispose of the corollaries. Corollary I is obvious. Corollary II is the result of combining Corollary I with Corollary I of Theorem 8A. As to Corollary III, if $\mathfrak{G}$ is a finite nilpotent group of class c, and if $\mathfrak{J}$ is any subgroup of $\mathfrak{G}$, the successive normalizers of $\mathfrak{J}$ sweep out $\mathfrak{G}$ in at most c steps; $\mathfrak{J}_a = \mathfrak{G}$ for $a \leqq c$. Thus, by Corollary I, G is nilpotent of class at most c.

As to Theorem 8B, it is certainly true for $i=0$, and we shall assume inductively that it is true for some fixed $i \geqq 0$, so that $\mathfrak{J}_i$ consists of all elements UR_a with U in $\mathfrak{J}$, a in Z_i. If T is in $\mathfrak{G}$ then $T = WR_x$ where W is in $\mathfrak{J}$ and $1T = x$. A necessary and sufficient condition that T be in $\mathfrak{J}_{i+1}$ is that to every element UR_a of $\mathfrak{J}_i$ there correspond an element VR_b of $\mathfrak{J}_i$ such that

$$(8.4) \qquad (WR_x)(UR_a) = (VR_b)(WR_x).$$

Assuming the truth of (8.4) we operate with both sides on 1 and derive $xU \cdot a = bW \cdot x$. Since b is in Z_i, so is bW, and this last equation implies $(xU)Z_i = Z_i x = xZ_i$. Thus xUL_x^{-1} must be in Z_i for every U of $\mathfrak{J}$, or, equivalently, x must be in Z_{i+1}. Hence $\mathfrak{J}_{i+1}$ is contained in the set of all elements WR_x with W in $\mathfrak{J}$, x in Z_{i+1}. Conversely let $T = WR_x$ where W is in $\mathfrak{J}$, x in Z_{i+1}. Then if UR_a is any element of $\mathfrak{J}_i$ we have $TUR_a = W_1R_y$ where $y = 1(TUR_a) = xU \cdot a$ and W_1 is in $\mathfrak{J}$. But, since x is in Z_{i+1}, $y = xU \cdot a = xb = cx$ with b, c in Z_i, and so $TUR_a = W_1R_{cx} = W_2R_cR_x = (W_2R_cW^{-1})(WR_x) = (VR_d)(WR_x)$ where W_2 and V are in $\mathfrak{J}$ and $d = cW^{-1}$ is in Z_i. Thus we have derived (8.4) with b replaced by d. It follows that $\mathfrak{J}_{i+1}$ not only is contained in but contains the set of all WR_x with W in $\mathfrak{J}$, x in Z_{i+1}. Hence our inductive proof goes through and Theorem 8B is true.

THEOREM 8C[13]. *A necessary and sufficient condition that a finite p-loop G be centrally nilpotent is that the associated group $\mathfrak{G}$ be a p-group.*

Proof. Since G and $\mathfrak{G}$ are together finite or infinite, we shall assume finiteness in what follows. If G is a centrally nilpotent p-loop, then by Corollary II to Theorem 8A, $\mathfrak{G}$ is a p-group. Conversely if $\mathfrak{G}$ is a p-group then G is a p-loop. Moreover $\mathfrak{G}$ is nilpotent; and hence, by Corollary III to Theorem 8B, G is centrally nilpotent.

The following sufficiency proof also seems worth recording, since it parallels closely the usual proof that a finite p-group is nilpotent. We say that two elements x, y of a loop G are conjugate in G if and only if $xU = y$ for some ele-

[13] Theorem 8C shows that the definition of a p-loop given earlier by the author (Bull. Amer. Math. Soc. Abstract 50-11-262) characterizes what is called here a finite centrally nilpotent p-loop.

ment U of the inner mapping group $\mathfrak{J}$. Thus the loop G may be partitioned into classes $x\mathfrak{J}$ of conjugate elements. If G is finite the number of elements in a class $x\mathfrak{J}$ divides the order of $\mathfrak{J}$, being the index in $\mathfrak{J}$ of the group $\mathfrak{F} \leqq \mathfrak{J}$ which leaves x fixed. A necessary and sufficient condition that x be in the centre Z of G is that $x\mathfrak{J} = x$, or that x be self-conjugate. Hence if G has finite order g and Z has (finite) order z we have

$$g = z + \sum h_i, \tag{8.5}$$

where each h is greater than 1 and represents the number of elements in some class. If $\mathfrak{G}$ is a p-group then $\mathfrak{J}$ is a p-group and G is a p-loop. But then g and each h_i is divisible by p; and so, by (8.5), z is divisible by p, Z is not the group of order one. It is easy to show (Albert [1]) that the group associated with G/Z is a quotient group of $\mathfrak{G}$, and thus the argument may be repeated. Therefore, since G is finite, it must be nilpotent.

9. **Finite centrally nilpotent p-loops.** The two preceding sections contain, usually as special cases, a large variety of theorems on finite centrally nilpotent p-loops, and we shall not repeat these. However we should like to make a few remarks linking our results with some of the introductory theory of P. Hall's fundamental paper [1] on finite p-groups, which has been the inspiration of most of the present work. If in §§1.1 to 1.4 of Hall's paper we agree to replace the word "group" everywhere by "loop," and to interpret "p-loop" as "centrally nilpotent p-loop," all the results and proofs of these sections remain valid, with three minor exceptions. These exceptions are: (1.14), which becomes meaningless since the normalizer of a subloop has not been defined (but compare the remarks on this topic in our §7); and (1.18), (1.19), which both become false for odd primes p. In fact we shall construct in Chapter III a centrally nilpotent p-loop of order p^2 which is not abelian.

We define an automorphism to be inner (as in §7) if and only if it lies in $\mathfrak{J}$.

Hall's enumeration principle (§1.4) remains valid since it depends only on the abelian p-group G/D, and the proof of his Theorem 1.51 is still good. Thus we may state the following theorem and refer the reader to Hall's paper for proof.

THEOREM 9A. *The number of subloops of order p^m of a centrally nilpotent p-loop of order p^n is congruent to* 1 (mod p) *for* $0 \leqq m \leqq n$.

The question of whether Kulakoff's theorem (Hall's Theorem 1.52) has an analogue for loops raises problems which are still unsolved. And indeed the interested reader will find a host of questions arising in regard to loop theory as he glances over the pages of any treatise on the theory of groups.

It might be added that, with some minor additions to the assumptions concerning the characteristic property π considered in §4, it is possible to define the notion of a π-commutator subloop $(H, K)_\pi$ of any two normal subloops H, K of a π-nilpotent loop G. In the present (central) case the commutator subloop (H, K) of two normal subloops H, K of G may be defined as the smallest subloop L of HK such that: (i) L is normal in G; (ii) each element of H/L commutes and associates (in G/L) with the elements of K/L, and conversely. There is no difficulty in proving the existence and uniqueness of $L=(H, K)$, but we have not attempted as yet to carry out the corresponding program suggested by Hall's paper.

10. **Associatral series.** In §§7–9 we have considered the situation which arises when "$a\pi G$" is interpreted to mean that a is in the centre C of the loop G. If C be replaced by any fixed one of the characteristic subloops A_λ, A_μ, A_ρ, or A of G we are led to the study of so-called left-associatral, middle-associatral, right-associatral or associatral series of G. It seems unnecessary to treat all of these types in detail, and we shall therefore restrict attention to left-associatral series.

Thus in the present instance "$a\pi G$" shall mean that

$$ax\cdot y = a\cdot xy \tag{10.1}$$

for all x, y of G. As noted in §4, equation (10.1) defines a characteristic property π. Moreover the postulates I and II for π-admissible loops are evidently satisfied by every loop G. The corresponding π-centre may appropriately be called the normal left associator of G. It is evident from the following theorem that postulates III and IV are also satisfied by every loop G.

THEOREM 10A. *If N is any normal subloop of a loop G, let $S(N, G)$ designate the set of all elements $nR_{x,y}L_n^{-1}$ with n in N, x, y in G, where as usual $R_{x,y}=R_xR_yR_{xy}^{-1}$. Then, for any normal subloop K of G, $(NK)/K$ is in the normal left associator of G/K if and only if $K\geqq S(N, G)$.*

Proof. A necessary and sufficient condition that $(nK\cdot xK)(yK)=(nK)\cdot(xK\cdot yK)$ for all n of N, x, y of G is that $(nx\cdot y)K=(nK)\cdot(xy\cdot K)$ or that $(nR_{x,y})K\cdot(xy\cdot K)=(nK)\cdot(xy\cdot K)$ or that $(nR_{x,y})K=nK$. But this is equivalent to $nR_{x,y}\in nK$ or to $nR_{x,y}L_n^{-1}\in K$ or to $S(N, G)\leqq K$. Hence the condition of Theorem 10A is necessary and sufficient that $(NK)/K$ be in the left associator of G/K. But since $(NK)/K$ is a normal subloop of G/K, the former will be in the *normal* left associator of the latter if and only if it is in the left associator. This completes the proof.

Since postulates I–IV are satisfied by every loop G, postulate V is trivially verified. Hence every loop is π-admissible in the present sense, and all the results of §4 may be asserted at once. Since moreover normal left associators are groups, it follows from §6 that every finite left-associatrally nilpotent or solvable loop has the strong Lagrange property (L′).

We leave the topic of associatral series at this stage, merely remarking that the results of §§7, 8 suggest many questions which are still unsettled. For example, does every maximum subloop of a finite left-associatrally nilpotent loop contain the left-associatrally derived loop?

11. **The autotopism group of a groupoid.** Let G be any groupoid and let $\mathfrak{P}$ be the group consisting of all permutations of G (§1). We shall here be concerned with the direct power $\mathfrak{P}_3 = \mathfrak{P} \times \mathfrak{P} \times \mathfrak{P}$, and with a certain important subgroup of $\mathfrak{P}_3$. We may think of $\mathfrak{P}_3$ as consisting of ordered permutation-triples

$$(11.1) \qquad \alpha = (U, V, W), \qquad \beta = (U_1, V_1, W_1)$$

under the multiplication

$$(11.2) \qquad \alpha\beta = (UU_1, VV_1, WW_1).$$

We may designate by βG the groupoid, isotopic to G, given by

$$(11.3) \qquad (xoy)W_1 = xU_1 \cdot yV_1.$$

(Here β is the permutation-triple (11.1), and $(\cdot)$ designates multiplication in G.) It follows that

$$(11.4) \qquad \alpha(\beta G) = (\alpha\beta)G$$

for all α, β of $\mathfrak{P}_3$, in the sense that both groupoids have the same product operation. In fact if $\alpha(\beta G)$ has operation $(*)$ then

$$(11.5) \qquad (x*y)W = (xU)o(yV),$$

whence, by (12.3), $(x*y)WW_1 = [(xU)o(yV)]W_1 = xUU_1 \cdot yVV_1$. Thus $(*)$ also designates multiplication in $(\alpha\beta)G$.

We define the element α of $\mathfrak{P}_3$ to be an *autotopism* of G if and only if $\alpha G = G$, or, equivalently, if and only if

$$(11.6) \qquad (xy)W = xU \cdot yV$$

for all x, y of G. If $\alpha G = G$ then, by (11.4), $G = \alpha^{-1}G$. Again, if also $\beta G = G$, then $(\alpha\beta)G = \alpha(\beta G) = \alpha G = G$. Hence the subset $\mathfrak{A}_3$ of $\mathfrak{P}_3$, consisting of all autotopisms of G, is a subgroup of $\mathfrak{P}_3$.

If T is a permutation of G it is evident from the definition that (T, T, T) is an autotopism of G if and only if T is an automorphism of G. Thus the automorphism group of G is isomorphic with a subgroup of the autotopism group.

The autotopism group of a groupoid G bears the same relation to the classification of the isotopes of G as the automorphism group of G bears to the classification of the isomorphs of G. In fact if $\alpha G = \beta G$, in the sense that both these isotopes of G have the same product operation, then $(\beta^{-1}\alpha)G = G$, so that $\beta^{-1}\alpha$ is an autotopism of G. We also note that if $\beta G = \theta(\alpha G)$ where $\theta = (T, T, T)$ gives an isomorphic mapping of αG into βG, then $\beta^{-1}\theta\alpha$ is an autotopism of G.

It would appear from these remarks that the autotopism group of a groupoid is worthy of careful study, and indeed we shall find such an investigation of considerable value in connection with the more special topics considered in Chapter II.

12. **The loop ring of a finite loop.** If G is a finite loop, written multiplicatively, and if F is an arbitrary field, we may regard the elements of G as a linearly independent basis for a linear vector space R over F. We may further define multiplication in R by use of the two-sided distributive law together with the definition of multiplication in G. Under these circumstances R is a linear non-associative algebra of a finite order over F, and is known as the *loop ring of G over F*. In Bruck [2, §7], loop rings (or rather the slightly more general quasigroup rings) were studied by means of the group $\mathfrak{G}$ associated with G. At this point we wish to indicate briefly a method of studying R by means of the inner mapping group $\mathfrak{I}$ of G. We assume a familiarity with the theory of linear algebras.

Definitions. If x is in G, the set of all elements xU with U in $\mathfrak{I}$ will be called the *class of elements* (of G) *conjugate to x*. This class may be designated briefly as $x\mathfrak{I}$.

The element $x_1+x_2+ \cdots +x_r$ of R, consisting of the sum of all distinct elements in the class $x\mathfrak{I}$, will be called *the sum of the class $x\mathfrak{I}$*, or, less explicitly, a *class sum*.

Theorem 12A. *Let C be the centre of R, where R is the loop ring of a finite loop G over a field F of characteristic prime to the order of the inner mapping group $\mathfrak{I}$ of G. Then C has order h, where h is the number of distinct conjugate classes of G. In fact, the h class sums of G form a linearly independent basis of R over F.*

Proof. Each element a of R has the form

$$a = \sum \alpha_r r \tag{12.1}$$

where r is in G and α_r is in F. If U is in $\mathfrak{I}$ we extend U to a linear mapping of R by the definition

$$aU = \sum \alpha_r(rU). \tag{12.2}$$

Now a is in the centre of R if and only if

$$ax\cdot y = a\cdot xy, \qquad xa\cdot y = x\cdot ay, \qquad xy\cdot a = x\cdot ya, \qquad ax = xa \tag{12.3}$$

for all x, y of R. But, since the elements of G form a linearly independent basis of R, there is no loss of generality in restricting x, y in (12.3) to be elements of G. It is then easy to show that a is in C if and only if

$$a = aU \tag{12.4}$$

for every U of $\mathfrak{I}$. If $\mathfrak{I}$ has order k it follows from (12.4) that $ka=\sum aU$ where the sum is over all distinct elements U of $\mathfrak{I}$. Since the characteristic of F is prime to k by hypotheses we have $a=k^{-1}\sum aU$, or, by (12.1),

$$a = \sum_r (k^{-1}\alpha_r) \sum_U (rU). \tag{12.5}$$

Now, for each fixed r of G, $\sum_U (rU) = ls$ where l is an integer and s is the sum of the class of elements conjugate to r. Hence it follows from (12.5) that every element of C is a linear combination of class sums. But, conversely, if s is a class sum and U is in $\mathfrak{J}$, $sU = s$, so C consists precisely of the vector space generated by the class sums.

If $s_1, s_2, \cdots, s_h$ are the class sums of the h distinct classes of G, no element of G appears as a summand in two distinct s_i, since the classes of G are obviously disjoint. Thus if $\alpha_1 s_1 + \alpha_2 s_2 + \cdots + \alpha_h s_h = 0$ for α_i in F it follows from the linear independence of the elements of G that $\alpha_i = 0$ for all i. Consequently the s_i form a linearly independent basis of C, and the latter is a linear (commutative and associative) algebra of order h. This completes the proof, and shows incidentally that a product of two class sums must be a sum of classes, as is otherwise evident.

THEOREM 12B. *Let G be a finite loop of order g, with h distinct conjugate classes. Let F be a field of characteristic zero or prime characteristic $p > g$, and let R be the loop ring of G over F. Then R is the direct sum of d simple algebras, where in general $d \leqq h$ but $d = h$ when F is algebraically closed.*

Proof. It has been shown elsewhere (Bruck [2, §7]) that, under the hypotheses of Theorem 12B, R is a direct sum $R = R_1 \oplus R_2 \oplus \cdots \oplus R_d$ of simple algebras R_i, and it may also be shown by the same methods that the centre C of R is a direct sum $C = C_1 \oplus C_2 \oplus \cdots \oplus C_d$ of simple, commutative associative algebras C_i. Moreover, if F is algebraically closed, each C_i must have order one. We shall assume these results, although a direct proof would be desirable.

Since the order of $\mathfrak{J}$ divides $g!$, our present hypotheses ensure the truth of Theorem 12A, and hence in particular we have $d \leqq h$. Moreover, if F is algebraically closed, it is clear from the preceding remarks that $d = h$. This completes the proof of Theorem 12B.

If in Theorem 12B we let F be the field of complex numbers and remember that loop rings of isotopic loops have essentially the same structure we see in particular that *two finite isotopic loops have the same number of distinct classes.* However a much better result is possible.

THEOREM 12C. *Let G be a loop, H any loop isotopic to G. Then to each class of conjugate elements of G there corresponds a class of conjugate elements of H with the same cardinal number. Moreover the set of all distinct classes of conjugate elements of G has the same cardinal number as the corresponding set for H.*

Proof. We merely sketch a method of proof. The reader may find it of interest to fill in the details. (i) H is isomorphic to a loop G_0 with the same elements and the same unit element as G, and such that (ii) G_0 and G have the same associated group $\mathfrak{G}$. (iii) G_0 and G have the same inner mapping group $\mathfrak{J}$. (iv) The classes of conjugate elements for G_0 are identical with those for G. As preface to a very simple example we may remark that Albert has shown [2, Theorem 16] that (aside from the cyclic groups) all loops of order 5 are isotopic. It is thus easily verified that every non-associative loop G of order 5 has exactly two classes and that the loop ring of G, over any field F of characteristic not 5, is a direct sum of F and a central simple non-associative algebra of order 4.

In the case of this example, and often in other cases, it is unnecessary to determine $\mathfrak{J}$ explicitly in order to find the conjugate classes of G. We need merely to observe that if $xu=uy$ or if $xu\cdot v=y\cdot uv$ then x and y are in the same class, and so on.

Chapter II. Loops with the inverse property

It seems proper to begin with the remark that here, as in the rest of Chapter II, all references to theorems and sections refer to Chapter II, unless the contrary is explicitly stated.

When the ideas of Chapter I are applied to loops with the inverse property (more briefly, to *I.P. loops*) a considerable simplification is achieved, apparently because of the fact that one may calculate freely with inverses, just as in the theory of groups. For example, the four associators A_λ, A_μ, A_ρ, and A all coincide, and hence we may speak unambiguously of the associator and of the notion of associatral admissibility (§3). On the other hand the theory is enriched in new directions. Indeed if G is an I.P. loop, the set of elements u such that $ux\cdot yu=(u\cdot xy)\cdot u$ for all x, y of G is a Moufang loop M, the *Moufang nucleus* of G (Theorem 4A). In terms of M we may introduce the new concept of *Moufang admissibility* and the corresponding notion of *Moufang nilpotency* (§5). Again, the set of elements v of G such that $v^2\cdot xy=vx\cdot vy$ for all x, y of G is a commutative Moufang loop C, the *Moufang centre* of G (Theorem 4C), through which we obtain the theory of *Moufang central series* (§6).

From these remarks it will perhaps be apparent that the special class of Moufang loops deserves a place of honour in the theory of I.P. loops. And indeed §1, devoted to groups for which the mapping $x\rightarrow x^3$ is an endomorphism into the centre, is included here only because of its importance for the structure theory of commutative Moufang loops. §2 contains the definitions of I.P. loops and Moufang loops, with a few known facts about their properties. §3 deals with the associator. In §4, by examining the structure of the autotopism group of an I.P. loop G, we uncover the relationship between G, M, and $C\leqq M$, and incidentally derive a number of results on Moufang loops. Of particular interest is the fact that *the inner mapping group of a commutative Moufang loop is a group of automorphisms.* We also give necessary and sufficient conditions that a like property hold for a noncommutative Moufang loop. As another by-product we may mention that the elements which commute with every element of a Moufang loop G form a subloop; this subloop is in fact the Moufang centre of G, which was defined somewhat differently above in the case of an arbitrary I.P. loop.

After brief sections on π-series (§§5–6) we turn to the study of Moufang loops. Theorems 7A, 7B sum up the facts previously obtained on Moufang loops, and Theorems 7C, 7D add further details to the theory of commutative Moufang loops, the latter giving necessary and sufficient conditions that a commutative Moufang loop be centrally nilpotent of class at most two.

In §8 we concentrate upon Moufang loops which possess an endomorphism $x \to x^3$ into the centre, and show in particular that this property holds for every isotope of a commutative Moufang loop; and hence, of course, for every subloop of such an isotope. When a Moufang loop G has this property, the system G_0 defined by $xoy = x^{-1}yx^2$ is a commutative Moufang loop (Theorem 8D). When G is also a group, G_0 is centrally nilpotent of class at most two (Theorem 8E), and in fact, every commutative Moufang loop which is centrally nilpotent of class at most 2 is either such a G_0 or a subloop of such a G_0 (Theorem 8F). In Theorem 8H we show how to construct a commutative Moufang loop with a normal subloop of index 3, and derive in particular the existence of commutative Moufang loops which are centrally nilpotent of class 3. (It might be pointed out here, since it becomes clear in the course of §9, that Theorem 8H essentially solves the general problem of extending a commutative Moufang loop to a commutative Moufang loop by use of a cyclic group, whether of order 3, as in the theorem, or of arbitrary order.) It is also proved in Theorem 8H that every Moufang loop, for which the mapping $x \to x^3$ is an endomorphism into its centre, is either an isotope of a commutative Moufang loop or a subloop of such an isotope. There is thus a most remarkable nontrivial relationship between the commutative Moufang loops and the Moufang loops for which $x \to x^3$ is an endomorphism into the centre.

In §9 we attack the commutative Moufang loops through a study of the generators $[x, y, z] = x^{-1}\{(xy \cdot z)(y^{-1}z^{-1})\}$ of the centrally derived loop. These are shown to be skew-symmetric, in the sense that interchange of any two of x, y, z replaces $[x, y, z]$ by its inverse (Theorem 9A). We develop the properties of the triples $[x, y, z]$ far enough to permit the explicit determination of the "freest" commutative Moufang loop G subject to the restrictions that G has n generators and is centrally nilpotent of class 2 (Theorem 9A). Finally, Theorem 9B generalizes previously published results of the author on the construction of non-commutative Moufang loops.

The well known theorem for groups, that the inner automorphism group of a group G is isomorphic to the central quotient group G/Z, is known to be false for loops. Nevertheless we are able to state an interesting analogue for Moufang loops. If G is a Moufang loop we designate by $\mathfrak{G}_\rho$ the group generated by the R_x with x in G, and by $\mathfrak{G}_\lambda$ the group similarly defined, in terms of the L_x. As before, $\mathfrak{G}=\{\mathfrak{G}_\rho, \mathfrak{G}_\lambda\}$ is the group associated with G, and $\mathfrak{J}$ is the inner mapping group of G. We show that $\mathfrak{K}=\mathfrak{J}\cap\mathfrak{G}_\rho=\mathfrak{J}\cap\mathfrak{G}_\lambda$ is a normal subgroup of $\mathfrak{J}$, and that the mapping $x\rightarrow\mathfrak{K}T_x$, where $T_x=R_xL_x^{-1}$, is a homomorphism of G upon the group $\mathfrak{J}/\mathfrak{K}$ (Theorem 10A). When G is a group this result reduces to the above-mentioned theorem on the inner automorphism group. We say that a Moufang loop G is of the first kind if $\mathfrak{G}_\rho=\mathfrak{G}_\lambda=\mathfrak{G}$, and of the second kind otherwise. Thus every Moufang loop of the second kind is homomorphic to a nontrivial group, and hence (assuming a suitable descending chain condition) is obtainable by a finite number of successive group-extensions from a loop of the first kind (Theorem 10B). It is also shown (Theorem 10D) that a finite Moufang p-loop is associatrally nilpotent if and only if it is centrally nilpotent.

1. **On a special class of groups.** It will be convenient to begin this chapter with some remarks on groups which possess an endomorphism $x\rightarrow x^3$ into the centre. With slight variations we follow a paper by F. Levi and B. L. van der Waerden [1] which deals with the Burnside groups in which $x^3=1$.

THEOREM 1A. *Let G be a group for which the mapping $x\rightarrow x^3$ is an endomorphism into the centre Z of G. Then*:

(i) $x^3=1$ *for every element x of the derived group* $G'=(G, G)$;

(ii) *G is nilpotent of class at most* 3: $(G, G, G, G)=1$;

(iii) *G' is an abelian group*;

(iv) *each element of G commutes with all its conjugates.*

Proof. (i) If

$$(1.1)\qquad (x, y) = x^{-1}y^{-1}xy$$

is a commutator we have $(x, y)^3=x^{-3}y^{-3}x^3y^3=x^{-3}x^3y^{-3}y^3=1$; but $G'=(G, G)$ is generated by the set of commutators (x, y).

(ii)–(iv). Since $(xy)^3=x^3y^3$ there results, for all x, y of G,

$$(1.2)\qquad xyx = y^{-1}x^{-1}y^{-1}\cdot x^3y^3.$$

Since x^3 is in Z for each x we find, by several uses of (1.2), that

$$\begin{aligned} x^{-1}y_1xy_2x^{-1} &= x^{-1}y_1x^{-1}\cdot x^{-1}y_2x^{-1}\cdot x^3 = (y_1^{-1}xy_1^{-1}\cdot x^{-3}y_1^3)\cdot(y_2^{-1}xy_2^{-1}\cdot x^{-3}y_2^3)\cdot x^3 \\ &= y_1^{-1}xy_1^{-1}\cdot y_2^{-1}xy_2^{-1}\cdot x^{-3}y_1^3y_2^3 = y_1^{-1}[x(y_2y_1)^{-1}x]y_2^{-1}\cdot x^{-3}y_1^3y_2^3 \\ &= y_1^{-1}[y_2y_1\cdot x^{-1}\cdot y_2y_1\cdot x^3(y_2y_1)^{-3}]y_2^{-1}\cdot x^{-3}y_1^3y_2^3 = y_1^{-1}y_2y_1x^{-1}y_2y_1y_2^{-1}. \end{aligned}$$

Thus

$$(1.3)\qquad x^{-1}y_1xy_2x^{-1} = y_1^{-1}y_2y_1x^{-1}y_2y_1y_2^{-1}$$

for all x, y_1, y_2 of G. From (1.3), on left-multiplication by x,

$$(1.4)\qquad y_1xy_2x^{-1} = xy_1^{-1}y_2y_1x^{-1}y_2y_1y_2^{-1},$$

whence in particular, with $y_1=y_2=y$,

$$y\cdot xyx^{-1} = xyx^{-1}\cdot y. \tag{1.5}$$

Thus *each element of G commutes with all its conjugates*. This proves (iv).

In view of (1.1), (1.5) may be rewritten, after left- and right-multiplication by y^{-1}, as $(x^{-1}, y^{-1})=(y, x^{-1})$. Therefore

$$(x, y) = (y^{-1}, x) = (x, y^{-1})^{-1}, \tag{1.6}$$

for all x, y of G. As usual we define

$$(x, y, z) = ((x, y), z), (x; y, z) = (x, (y, z), (x,\ y; z, w) = ((x, y), (z, w)). \tag{1.7}$$

Then, in detail,

$$(a, b, c) = b^{-1}a^{-1}bac^{-1}a^{-1}b^{-1}abc = b^{-1}a^{-1}(b\cdot ac^{-1}a^{-1}\cdot b^{-1}\cdot a\cdot b)c.$$

We may now apply (1.3) to the product in parentheses, using $x=b^{-1}$, $y_1=ac^{-1}a^{-1}$, $y_2=a$. There results

$$\begin{aligned}(a, b, c) &= b^{-1}a^{-1}(aca^{-1}\cdot a\cdot ac^{-1}a^{-1}\cdot b\cdot a\cdot ac^{-1}a^{-1}\cdot a^{-1})c\\ &= b^{-1}\cdot cac^{-1}a^{-1}\cdot b\cdot a^2c^{-1}a^{-2}c = b^{-1}\cdot(c^{-1}, a^{-1})\cdot b\cdot(a, c),\end{aligned}$$

since a^3 is in Z. But, by two uses of (1.6), $(c^{-1}, a^{-1})=(a, c^{-1})=(a, c)^{-1}$, and hence we have $(a, b, c)=(b; a, c)=((a, c)^{-1}, b)=(c, a, b)$, or

$$(x, y, z) = (y; x, z) = (z, x, y) \tag{1.8}$$

for all x, y, z of C. Thus, in particular, (x, y, z) *is invariant under cyclic permutations of* x, y, z.

If we define, as usual,

$$(x, y, z, w) = ((x, y, z), w) \tag{1.9}$$

it follows from (1.7), by two applications of (1.8), that

$$(x, y; z, w) = (z, w, x, y) = (x; z, w, y). \tag{1.10}$$

From (1.10), and the above remark concerning (x, y, z), we see that $(x, y; z, w)$ is invariant under cyclic permutations both of z, w, x and of z, w, y, and hence under the alternating group on x, y, z, w. Thus, using the even permutation $(xz)(yw)$, we have $(x, y; z, w)^{-1}=(z, w; x, y)^{-1}=(x, y; z, w)$ or $1=(x, y; z, w)^2$. Hence, by (i),

$$(x, y; z, w) = (x, y; z, w)^3 = 1. \tag{1.11}$$

From (1.10) and (1.11) it follows that $(z, w, x, y)=1$ for all z, w, x, y of G. Thus $(G, G, G, G)=1$, or (G', G) is in Z; in other words G is nilpotent of class at most 3. This proves (ii).

The main object of the Levi-van der Waerden paper [1] is the proof of the following theorem, which we shall be content merely to state.

THEOREM 1B. *There exists a group G with the following properties:*

(i) $x^3 = 1$ *for every* x *of* G;

(ii) G *has* n *generators, where* $n \geqq 3$ *is a positive integer*;

(iii) G, *its derived group* G', *and its centre* Z *have respective orders* 3^e, 3^f, 3^g *where*

$$(1.12) \qquad e = C_{n,1} + C_{n,2} + C_{n,3}, \qquad f = C_{n,2} + C_{n,3}, \qquad g = C_{n,3};$$

(iv) G *is nilpotent of class* 3;

(v) G, G', Z *and* 1 *are the only characteristic subgroups of* G;

(vi) *Every group* H *with properties* (i) *and* (ii) *is a homomorphic image of* G.

It is of course evident that if a non-abelian group G with two generators a, b satisfies (i) of Theorem 1B (or even the less restrictive hypotheses of Theorem 1A) the commutator (a, b) lies in Z and hence G has class 2.

2. **Loops with the inverse property.** A loop G is said to be a *loop with the inverse property* (or, more briefly, an I.P. loop) if and only if, to every element x of G, there corresponds a unique element x^{-1} of G such that the equations

$$(2.1) \qquad x^{-1} \cdot xy = y, \qquad yx \cdot x^{-1} = y$$

hold for every y of G. For various methods of constructing I.P. loops, and for a detailed study of the more general subject of I.P. quasigroups, the reader is referred to a previous paper (Bruck [1]). From (2.1) with $y = 1$ we see that

$$(2.2) \qquad x^{-1}x = xx^{-1} = 1,$$

and hence also that

$$(2.3) \qquad (x^{-1})^{-1} = 1.$$

Moreover the mapping $x \rightarrow x^{-1}$ is an anti-automorphism of the I.P. loop G:

$$(2.4) \qquad (xy)^{-1} = y^{-1}x^{-1}.$$

In fact, if $xy = z$, then, by successive uses of (2.1), $y = x^{-1}z$, $x^{-1} = yz^{-1}$, $z^{-1} = y^{-1}x^{-1}$; but this last equation is equivalent to (2.4). It will be convenient to have two lemmas concerning special types of I.P. loops.

LEMMA 2A. *If the equation*

$$(2.5) \qquad (x \cdot yz)x = xy \cdot zx$$

holds for all x, y, z *of the loop* G, *then* G *is an I.P. loop.*

Proof. From (2.5) with $y = 1$ we derive

$$(2.6) \qquad xz \cdot x = x \cdot zx$$

for all x, z of G. If for each x of G we define x^{-1} to be the unique solution of the equation $x \cdot x^{-1} = 1$ it follows from (2.6) with $z = x^{-1}$ that $x = x \cdot x^{-1}x$ or $x^{-1}x = 1$.

Thus (2.2), and hence (2.3), holds for all x of G. Now we set $x=y^{-1}$ in (2.5) and derive $(y^{-1}\cdot yz)y^{-1}=zy^{-1}$ or $y^{-1}\cdot yz=z$ for all y, z of G. Therefore the first equation of (2.1) holds in G. Again, (2.5) and (2.6) together imply $x\cdot(yz\cdot x)=xy\cdot zx$, from which with $x=z^{-1}$ we derive $z^{-1}\cdot(yz\cdot z^{-1})=z^{-1}y$ or $yz\cdot z^{-1}=y$, which is essentially the second equation of (2.1). This completes the proof.

LEMMA 2B. *If the equation*

$$x(y\cdot zy) = (xy\cdot z)y \tag{2.7}$$

holds for all x, y, z of the loop G, then G is an I.P. loop.

Proof. From (2.7) with $x=1$ follows $y\cdot zy=yz\cdot y$, or (2.6), and thus (2.2), (2.3) as before. Then (2.7) with $z=y^{-1}$ yields essentially the second equation of (2.1). Again, (2.7) with $x=y^{-1}$ yields $y^{-1}(y\cdot zy)$, which, when zy is replaced by z, is essentially the first equation of (2.1). This completes the proof.

DEFINITION. A loop G is Moufang if and only if equation (2.7) is valid for all x, y, z of G.

It follows from the definition that a Moufang loop has the inverse property, as indeed is well known. (For some historical remarks see Bruck [1, p. 44].) G. Bol [1] has shown that, in a loop G, the defining relation (2.7) implies the defining relation (2.5), and, in a letter to the author, D. C. Murdoch has raised a question as to the converse proposition. This is in fact also valid, but it will be convenient to defer the proof, since both results fall out as by-products of later work on autotopisms (Corollary 2 to Lemma 4A).

For proof of the following theorem we refer the reader to a paper by R. Moufang [1].

THEOREM 2A. *Let G be a Moufang loop. Then*

(i) *every two elements x, y of G generate a group*;

(ii) *if three elements x, y, z of G are associative in some order* (*say $x\cdot yz=xy\cdot z$*) *then $\{x, y, z\}$ is a group.*

In the present chapter we shall make frequent use of the various consequence of Theorem 2A and of (i) in particular. It should be observed that (i) obviates all necessity for the use of brackets in products formed from one or two elements. Thus for Moufang loops the power x^n (for integral n) is unambiguous, and so is the commutator

$$(x, y) = x^{-1}y^{-1}xy. \tag{2.8}$$

As another obvious consequence of (i) we note that every two elements of a commutative Moufang loop generate an abelian group. Hence we have:

COROLLARY. *If G is a commutative Moufang loop, not an abelian group, then G has at least three generators.*

Moreover Bol [1] gives an example of a non-abelian commutative Moufang loop (of order 81) with exactly three generators.

We conclude this section with an easily proved assertion which may possess some interest for the reader.

THEOREM 2B. *Let G be a groupoid with unit* 1. *Suppose that to every x of G there corresponds at least one element x', and at least one element x'', such that*

$$x' \cdot xy = x \cdot x'y = y, \qquad yx \cdot x'' = yx'' \cdot x = y \tag{2.9}$$

hold for every y of G. Then G is a loop with the inverse property.

3. **The associator of an I.P. loop.** The characteristic subloops A_λ, A_μ, A_ρ and $A = A_\lambda \cap A_\mu \cap A_\rho$ of the arbitrary loop G have been defined in §§1, 2 of Chapter I. The following theorem shows that all of these coincide for a loop with the inverse property.

THEOREM 3A. *If G is an I.P. loop, if a is a fixed element of G, and if one of the following equations holds for all x, y of G, then each of the others holds as well.*

$$ax \cdot y = a \cdot xy; \tag{3.1}$$

$$xa \cdot y = x \cdot ay; \tag{3.2}$$

$$xy \cdot a = x \cdot ya. \tag{3.3}$$

Proof. (3.1) *is equivalent to* (3.3). From (3.1), by taking inverses, we find $y^{-1} \cdot x^{-1}a^{-1} = y^{-1}x^{-1} \cdot a^{-1}$, or (when y^{-1}, x^{-1} are replaced by x, z), $x \cdot za^{-1} = xz \cdot a^{-1}$. Setting $z = ya$ we get $xy = (x \cdot ya)a^{-1}$ and $xy \cdot a = x \cdot ya$. Thus (3.1) implies (3.3), and (obviously) conversely.

(3.1) *is equivalent to* (3.2). We multiply each side of (3.1) on the left by $(ax)^{-1} = x^{-1}a^{-1}$, whence $y = x^{-1}a^{-1} \cdot (a \cdot xy)$. In this relation replacement of y by $x^{-1} \cdot a^{-1}y^{-1}$ gives $x^{-1} \cdot a^{-1}y^{-1} = x^{-1}a^{-1} \cdot y^{-1}$, whence, by inversion, $ya \cdot x = y \cdot ax$. Thus (3.1) implies (3.2). But conversely, multiplication of (3.2) on the right by $(ay)^{-1} = y^{-1}a^{-1}$ yields $(xa \cdot y)(y^{-1}a^{-1}) = x$, whence replacement of x by $xy^{-1} \cdot a^{-1}$ gives $x \cdot y^{-1}a^{-1} = xy^{-1} \cdot a^{-1}$; from which by inversion $ay \cdot x^{-1} = a \cdot yx^{-1}$. This completes the proof.

The terms *associator* and *normal associator* are thus unambiguous for I.P. loops, and the various notions of associatral series (§10 of Chapter I) now coincide. But an even better situation exists for Moufang loops.

THEOREM 3B. *The associator A of a Moufang loop G is a* (*characteristic*) *normal subloop of G.*

Proof. If a is in A we have $aR_{x,y} = a$ by (3.1) and $a = aL_{y,x}$ by (3.3). But the inner mapping group of G is known to be generated by the set of all $R_{x,y}$, $L_{x,y}$ and T_x, where $T_x = R_x L_x^{-1}$, $aT_x = x^{-1} \cdot ax$. Thus, by virtue of Theorem 3A, it is only necessary to establish the equation

$$y \cdot z \cdot (x^{-1}ax) = yz \cdot x^{-1}ax \tag{3.4}$$

for all a of A and x, y, z of G. We do this by easy stages. Now, by (2.6) and the fact that a is in A, $xy\cdot xa=(xy\cdot x)a=(x\cdot yx)\cdot a=x\cdot(yx\cdot a)$, or

$$xy\cdot xa = x\cdot(yx\cdot a). \tag{3.5}$$

By (2.5) and (3.5), $z(x^{-1}ax)=(x\cdot x^{-1}z)(x^{-1}a\cdot x)=[x\cdot(x^{-1}z\cdot x^{-1}a)]x=[x\{x^{-1}\cdot(zx^{-1}\cdot a)\}]x=(zx^{-1}\cdot a)x=zx^{-1}\cdot ax$, or

$$z(x^{-1}ax) = zx^{-1}\cdot ax. \tag{3.6}$$

By (2.5) and (2.6), $x[(x^{-1}y)(zx^{-1}\cdot a)]=x[(x^{-1}y\cdot zx^{-1})a]=x[\{x^{-1}\cdot(yz\cdot x^{-1})\}]a=(yz\cdot x^{-1})a$, or

$$x[(x^{-1}y)(zx^{-1}\cdot a)] = (yz\cdot x^{-1})a. \tag{3.7}$$

By (3.6), (2.5), (3.7) and (3.6), $y[z\cdot(x^{-1}ax)]=y(zx^{-1}\cdot ax)=(x\cdot x^{-1}y)[(zx^{-1}\cdot a)x]=\{x[(x^{-1}y)(zx^{-1}\cdot a)]\}x=[(yz)\cdot x^{-1})a]x=(yz\cdot x^{-1})(ax)=yz\cdot x^{-1}ax$. Thus (3.4) is established.

The following example shows the existence of a loop of order 6 (not an I.P. loop!) in which the left associator (elements 1, 2) has order 2 and the middle and right associators each have order 1. (Note that the left associator is the *only* proper subloop.)

(3.8)

·	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	3	6	5
3	3	6	5	1	4	2
4	4	5	6	2	3	1
5	5	3	1	6	2	4
6	6	4	2	5	1	3

The loop (3.8) may also be used to illustrate the fact, so often reiterated in Chapter I, that characteristic subloops need not be normal.

4. The autotopism group of an I.P. loop.

The notion of an autotopism (U, V, W) of a loop G has been introduced in §11 of Chapter I. In the present connection it will be convenient to introduce the permutation J of the I.P. loop G, defined by

$$xJ = x^{-1}. \tag{4.1}$$

LEMMA 4A. *Let (U, V, W) be an autotopism of the I.P. loop G. Then (JUJ, W, V) and (W, JVJ, U) are also autotopisms of G.*

COROLLARY 1. *In addition, (V, JWJ, JUJ), (JWJ, U, JVJ) and (JVJ, JUJ, JWJ) are autotopisms of G.*

COROLLARY 2. *For an I.P. loop G the defining relations* (2.5) *and* (2.7) *are equivalent; either characterizes a Moufang loop.*

Proof. By hypothesis we have

$$xU\cdot yV = (xy)W \tag{4.2}$$

for all x, y of G. Right-multiplication of (4.2) by $(yV)^{-1}=yVJ$ gives $xU=(xy)W\cdot yVJ$, whence, with x, y respectively replaced by xy, $y^{-1}=yJ$, we derive $(xy)U=xW\cdot yJVJ$. Thus (W, JVJ, U) is an autotopism. Again, left multiplication of (4.2) by xUJ and replacement of x, y respectively by xJ, xy gives $(xy)V=xJUJ\cdot yW$, whence (JUJ, W, V) is an autotopism. This proves the lemma. It should be noted that we now have a process of deriving new autotopisms from a given one (U, V, W): interchange one of the first two elements with the last, and transform the remaining element by $J=J^{-1}$. Corollary 1 results from repetitions of this process. As to Corollary 2, the defining relation (2.5), or $(x\cdot yz)x=xy\cdot zx$, holds for the I.P. loop G if and only if (L_x, R_x, L_xR_x) is an autotopism of G for all x of G. When this is true it follows from Lemma 4A that (JL_xJ, L_xR_x, R_x) is an autotopism of G, and so $(xy^{-1})^{-1}\cdot(xz\cdot x)=yz\cdot x$ or $yx^{-1}\cdot(xz\cdot x)=yz\cdot x$ in G. The latter equation, with y replaced by yx (and with $xz\cdot x$ replaced by $x\cdot zx$ by virtue of (2.6)), yields (2.7) with the roles of x and y interchanged. Since each step is clearly reversible, the proof of Corollary 2 is complete.

LEMMA 4B. *Let $u=1U$, $v=1V$, $w=1W$ where (U, V, W) is an autotopism of the loop G. Then $uv=w$, and*

$$V^{-1}W = L_u, \qquad U^{-1}W = R_v. \tag{4.3}$$

Proof. From (4.2) with $x=1$ we derive $u\cdot yV=yW$. If $y=1$ we have $uv=w$. In any case $VL_u=W$, or $L_u=V^{-1}W$. Similarly from (4.2) with $y=1$, $xU\cdot v=xW$ or $UR_v=W$, $R_v=U^{-1}W$.

For the next result it is convenient to note that the equation $(xy)^{-1}=y^{-1}x^{-1}$ for I.P. loops yields $R_yJ=JL_{y^{-1}}=JL_y^{-1}$, or indeed

$$JR_xJ = L_x^{-1}, \qquad JL_xJ = R_x^{-1}. \tag{4.4}$$

We have of course used the fact that, for example, $yR_xR_{x^{-1}}=yx\cdot x^{-1}=y$ or $R_xR_x^{-1}=I$, $R_{x^{-1}}=R_x^{-1}$.

LEMMA 4C. *Let (U, V, W) be an autotopism of the I.P. loop G. Then, in the notation of Lemma* 4B, *(L_u, R_u, L_uR_u) is an autotopism of G; that is,*

$$ux\cdot yu = (u\cdot xy)u \tag{4.5}$$

for all x, y of G.

DEFINITION. An element u of the I.P. loop G which satisfies (4.5) shall be called a Moufang element of G.

COROLLARY. *The elements u, u^{-1}, v, v^{-1}, w, w^{-1} are all Moufang elements of G.*

Proof of Lemma 4C. By Lemma 4A and Corollary 1, and the fact that the autotopisms form a group, it follows that the permutation triple

$$(V, JWJ, JUJ)^{-1}(W, JVJ, U) = (V^{-1}W, JW^{-1}VJ, JU^{-1}JU)$$

is an autotopism of G. By (4.3), $V^{-1}W=L_u$, and so, by (4.4), $JW^{-1}VJ=(JV^{-1}WJ)^{-1}=(JL_uJ)^{-1}=R_u$. Thus, if we write $JU^{-1}JU=T$, we have that (L_u, R_u, T) is an autotopism, or that

$$ux\cdot yu = (xy)T \tag{4.6}$$

for all x, y of G. From (4.6) with $y=1$ we have $ux\cdot u=xT$ or $T=L_uR_u$. This completes the proof of Lemma 4C. As to the corollary, we need only to refer to Lemma 4A and Corollary 1, and to note that $1JUJ=uJ=u^{-1}$, $1W=w$, $1V=v$, $1JWJ=w^{-1}$, $1JVJ=v^{-1}$.

THEOREM 4A. *Let M be the set of all Moufang elements of the I.P. loop G. Then M is a (characteristic) subloop of G, and, moreover, M is a Moufang loop, which we shall call the Moufang nucleus of G.*

Proof. If u is a Moufang element, then $(L_u, R_u, L_uR_u)^{-1}=(L_u^{-1}, *, *)$ is an autotopism and hence, by Lemma 4C, $1L_u^{-1}=u^{-1}$ is a Moufang element[14]. If v is also a Moufang element, then $(L_v, R_v, L_vR_v)(L_u, R_u, L_uR_u)=(L_vL_u, *, *)$ is an autotopism, and so again $1L_vL_u=uv$ is a Moufang element. Thus M is a subloop of G. That M is Moufang should be obvious from (4.5), Corollary 2 to Lemma 4A, and the definition of a Moufang loop (§2).

LEMMA 4D. *Let u, v be Moufang elements of the I.P. loop G. Then*

$$L_{uv} = \overset{-1}{R_u}L_vR_uL_u, \qquad R_{uv} = \overset{-1}{L_v}R_uL_vR_v. \tag{4.7}$$

Proof. The product $(L_u, R_u, L_uR_u)(L_v, R_v, L_vR_v)$ is an autotopism, so

$$xL_uL_v\cdot yR_uR_v = (xy)L_uR_uL_vR_v \tag{4.8}$$

for all x, y of G. From (4.8) with $y=1$ we derive $L_uL_vR_{uv}=L_uR_uL_vR_v$, or $R_{uv}=L_v^{-1}R_uL_vR_v$. Moreover from (4.5) with $x=1$ we have $u\cdot yu=uy\cdot u$, whence, for any Moufang element u,

$$R_uL_u = L_uR_u. \tag{4.9}$$

Finally, from (4.8) with $x=1$, $R_uR_vL_{vu}=L_uR_uL_vR_v$, or, by use of (4.9), $L_{vu}=R_v^{-1}L_uR_vL_v$. But this is the first equation of (4.7), with u and v interchanged.

COROLLARY. *In a Moufang loop G, equations (4.7) hold for all u, v of G. Moreover Albert's groups $\mathfrak{G}_\lambda$, $\mathfrak{G}_\rho$ are normal subgroups of the associated group $\mathfrak{G}$.*

[14] Here and later we write asterisks (*) in place of elements in which we have no immediate interest.

For example, $\mathfrak{G}_\lambda$ is defined to be the group generated by the L_x with x in G; but $R_u^{-1}L_vR_u=L_{uv}L_u^{-1}$ by (4.7), and it follows that $T^{-1}\mathfrak{G}_\lambda T\leqq\mathfrak{G}_\lambda$ for every T of $\mathfrak{G}$. Similarly $\mathfrak{G}_\rho=\{R_x;\ x\in G\}$, but $L_v^{-1}R_uL_v=R_{uv}R_v^{-1}$, and so $T^{-1}\mathfrak{G}_\rho T\leqq\mathfrak{G}_\rho$ for every T of $\mathfrak{G}$.

LEMMA 4E. *Let (U, V, W) be an autotopism of the I.P. loop G, with $1U=u$, $1V=v$, $1W=w=uv$. Then if $u=1$, a necessary and sufficient condition that U be an automorphism of G is that $v=w$ lie in the associator of G. Similarly, if $v=1$, a necessary and sufficient condition that V be an automorphism of G is that $u=w$ lie in the associator; and, if $w=1$, a necessary and sufficient condition that W be an automorphism of G is that $u=v^{-1}$ lie in the associator.*

Proof. We shall prove only the first statement. (The others can be obtained by use of Lemma 4A.) Since $u=1$ it follows from (4.3) that $V=W=UR_v$. Thus

$$(4.10)\qquad (xU)\cdot(yU\cdot v) = (xy)U\cdot v.$$

Now if v is in the associator, the left-hand side of (4.10) may be written as $(xU\cdot yU)v$. Thus $xU\cdot yU=(xy)U$, or U is an automorphism. Conversely, if U is an automorphism, the right-hand side of (4.10) may be written as $(xU\cdot yU)v$. Thus, when x, y are replaced by xU^{-1}, yU^{-1}, we have $x\cdot yv=xy\cdot v$, whence v is in the associator.

In Chapter I it was shown that the inner mapping group $\mathfrak{J}$ of a loop G could be generated by the set of all permutations

$$(4.11)\qquad L_{x,y} = L_xL_yL_{yx}^{-1},\qquad R_{x,y} = R_xR_yR_{xy}^{-1},\qquad T_x = R_xL_x^{-1}$$

with x, y in G. The following theorem therefore yields considerable information about the inner mapping group of a Moufang loop.

THEOREM 4B. *Let G be an I.P. loop with associator A, and let u, v be Moufang elements of G. Then a necessary and sufficient condition that T_u, $R_{u,v}$ or $L_{u,v}$ be an automorphism of G is that u^3, $v^{-1}u^{-1}vu$ or $uvu^{-1}v^{-1}$ respectively lie in A.*

COROLLARY 1. *A necessary and sufficient condition that the inner mapping group of a Moufang loop G should be a group of automorphisms of G is that x^3 and $(x, y)=x^{-1}y^{-1}xy$ lie in the associator of G, for all x, y of G.*

COROLLARY 2. *If G is a commutative Moufang loop the mapping $x\rightarrow x^3$ yields an endomorphism of G into its centre Z. Moreover the inner mapping group is a group of automorphisms of G.*

Proof. As a matter of convenience let us define A_u by

$$(4.12)\qquad A_u = (L_u, R_u, L_uR_u).$$

Since A_u is an autotopism, so, by Lemma 3A, is $B=(L_uR_u, L_u^{-1}, L_u)$. Thus $A_uB=(L_u^2R_u, T_u, *)$ is an autotopism with $1T_u=1$, and hence, by Lemma 4E,

T_u is an automorphism if and only if $1L_u{}^2R_u=u^3$ is in the associator. Again, $A_uA_vA_{uv}{}^{-1}=(L_uL_vL_{uv}{}^{-1}, R_{u,v}, *)$ is an autotopism with $1R_{u,v}=1$, and hence $R_{u,v}$ is an automorphism if and only if $1L_uL_vL_{uv}{}^{-1}=v^{-1}u^{-1}vu$ lies in A. Finally, $A_uA_vA_{vu}{}^{-1}=(L_{u,v}, R_uR_vR_{vu}{}^{-1}, *)$ is an autotopism with $1L_{u,v}=1$, and hence $L_{u,v}$ is an automorphism if and only if $1R_uR_vR_{vu}{}^{-1}=uvu^{-1}v^{-1}$ is in A. This completes the proof of Theorem 4B, and Corollary 1 follows immediately. In the case of Corollary 2, $x^{-1}y^{-1}xy=1$ for all x, y and so $R_{x,y}=L_{x,y}$ is an automorphism. But also $T_x=R_xL_x{}^{-1}=I$ is an automorphism, so x^3 lies in the associator, now become the centre. The fact that $(xy)^3=x^3y^3$ follows from commutativity and Theorem 2A.

THEOREM 4C. *If u is a fixed element of an I.P. loop G, a necessary and sufficient condition that*

$$u^2\cdot xy = ux\cdot uy \tag{4.13}$$

for all x, y of G is that u be a Moufang element which commutes with every element of G;

$$ux = xu, \qquad ux\cdot yu = (u\cdot xy)u \tag{4.14}$$

for all x, y of G. The set of all such u forms a (characteristic) commutative Moufang subloop C of G, which we shall call the Moufang centre of G.

COROLLARY 1. *If G is a Moufang loop, the set of all elements which commute with every element of G is a (characteristic) subloop, the Moufang centre of G.*

COROLLARY 2. *The inner mapping group of the Moufang centre C of an I.P. loop G is the homomorphic image of a group of automorphisms of G.*

Proof. From (4.13) with $y=1$, $u^2\cdot x=ux\cdot u$. From (4.13) with $x=1$, $u^2\cdot y=u\cdot uy$. Thus we obtain $u^2\cdot x=ux\cdot u=u\cdot ux$, whence it is clear that u commutes with every element of G and also that (4.13) may be replaced by the second equation of (4.14). From the first equation of (4.14), $L_u=R_u$, and thus also $L_{u^{-1}}=R_{u^{-1}}$. If v is another Moufang element with $L_v=R_v$, then by (4.7), $L_{uv}=L_{vu}=R_v{}^{-1}L_uR_vL_v=L_v{}^{-1}R_uL_vR_v=R_{uv}$, so that uv has the same property. Corollary 1 is immediate, and Corollary 2 follows from Theorem 4B. In fact $R_{u,v}=L_{u,v}$ is an automorphism of G for all u, v of C; and of course $T_u=I$.

We are forced to leave unsolved the problem of completely determining the autotopism group of an arbitrary I.P. loop. We have encountered three special types of autotopism: (1) (T, T, T), where T is an automorphism; (2) (L_u, R_u, L_uR_u), where u is a Moufang element; and the autotopisms obtainable from this by the method of Lemma 4A; (3) (I, R_a, R_a), where I is the identity permutation and a is an associator element; and the autotopisms obtainable from this by Lemma 4A. (Type (3) was implicitly treated in Lemma 4E.) In the case of a group it is readily seen that the three types suffice to generate the autotopism group, but the question remains open as to whether the same situation prevails for every I.P. loop. The assumption of commutativity, however, leads to an affirmative answer.

THEOREM 4D. *The autotopism group of a commutative I.P. loop G is generated by the autotopisms of the three types described in the preceding paragraph. More precisely, every autotopism of G has the form $\alpha\beta\gamma$ where α, β, γ are autotopisms of types* (1), (2) *and* (3) *respectively.*

Proof. Since G is commutative we may write $L_x = R_x$ for each x. If (U, V, W) is an autotopism, it follows from (4.2), by interchange of x and y, that (V, U, W) is also an autotopism. Thus, using (4.3), we see that $(U, V, W)^{-1}\cdot(V, U, W) = (U^{-1}V, U^{-1}U, I) = (R_vR_u^{-1}, R_uR_v^{-1}, I)$ is an autotopism. Application of Lemma 4E shows that the element $a = 1R_vR_u^{-1} = vu^{-1}$ lies in the associator (here the centre) of G. Thus $v = au = ua$ and so $w = uv = au^2 = u^2a$. If we now define $\gamma = (I, R_a, R_a)$, $\beta = (R_u, R_u, R_u^2)$, so that β, γ are autotopisms, we have $(U, V, W)\gamma^{-1}\beta^{-1} = (U', V', W')$ where $U' = UR_u^{-1}$, $V' = VR_a^{-1}R_u^{-1}$, $W' = WR_a^{-1}R_u^{-2}$ and hence $1U' = 1V' = 1W' = 1$. It follows at once that $U' = V' = W' = T$ where T is some automorphism of G. Thus, finally, if $\alpha = (T, T, T)$, we have $(U, V, W) = \alpha\beta\gamma$ as stated.

5. **Moufang series for I.P. loops.**

Let the characteristic property π be the "Moufang property" expressed as follows: u has property π with respect to the loop G if and only if

$$ux\cdot yu = (u\cdot xy)\cdot u \tag{5.1}$$

for all x, y of G. We now consider the postulates laid down in §4 of Chapter I.

THEOREM 5A. *Every I.P. loop G is Moufang-admissible, in the sense of equation* (5.1).

Proof. Postulate (I) holds, since G_π is the Moufang nucleus of G—the set of all Moufang elements. Thus the π-centre will be a Moufang loop. Postulate II is trivially verified. As to postulate III, let N be a normal subloop of G and designate by $S(N)$ the set of all elements p of G such that

$$(nx\cdot yn)p = (n\cdot xy)n \tag{5.2}$$

for some n in N and x, y in G. Since N is normal in G, $(n\cdot xy)\cdot n = xy\cdot a$ and $(nx\cdot yn)p = (xy\cdot b)p = xy\cdot cp$ for some a, b, c in N. Thus $xy\cdot a = xy\cdot cp$, $a = cp$, p is in N, and $S(N)$ is a subset of N. If K is a normal subloop of G, a necessary and sufficient condition that $(NK)/K$ be in the Moufang nucleus of G/K is that

$$(nx\cdot yn)K = [(n\cdot xy)n]K \tag{5.3}$$

for all n of N, x, y of G; or, equivalently, that the elements p defined by (5.2) be in K. Hence the set $S(N)$, defined as above, satisfies the demands of postulate III. Finally, postulates IV and V are obviously satisfied.

6. **Moufang central series for I.P. loops.** This time u will be said to have property π with respect to the loop G if and only if, for all x, y of G,

$$u^2 \cdot xy = ux \cdot uy. \tag{6.1}$$

Equivalently, u must satisfy (5.1) and commute with every element of G.

Theorem 6A. *Every I.P. loop G is Moufang-centrally admissible in the sense of equation* (6.1).

Proof. G_π is the Moufang centre of G. If N is a normal subloop of G, $S(N)$ is defined to be the set of all elements p of G such that

$$(n^2 \cdot xy)p = nx \cdot ny. \tag{6.2}$$

It is readily seen, as in the previous section, that the five postulates for π-admissibility are satisfied.

As noted in Corollary 1 to Theorem 4C, the Moufang centre of a Moufang loop G consists of those elements u of G which commute with every element of G. Thus for Moufang loops equation (6.1) may be replaced by

$$ux = xu, \tag{6.3}$$

and, correspondingly, (6.2) may be replaced by $nx \cdot p = xn$ or

$$p = (x, n) = x^{-1}n^{-1}xn. \tag{6.4}$$

Thus we have the following theorem.

Theorem 6B. *Let G be a Moufang loop, N a normal subloop of G. Designate by $C(N, G)$ the intersection of all normal subloops of G which contain every commutator (x, n) with x in G, n in N. Then $C(N, G)$ is a subloop of N and a normal subloop of G. Moreover, if K is a normal subloop of G, NK/K is in the Moufang centre of G/K if and only if $K \geqq C(N, G)$.*

7. **Structure theorems for Moufang loops.** Aside from Theorem 2A (Moufang's theorem) we have obtained a number of results on Moufang loops more or less incidentally to the course of the preceding study of I.P. loops. It will be convenient to list these here in the form of two theorems.

Theorem 7A. *If G is a Moufang loop, then:*

(i) *G is characterized by either of the laws $xy \cdot zx = (x \cdot yz) \cdot x$, $x(y \cdot zy) = (xy \cdot z)y$. In particular G has the inverse property* (*Lemmas* 2A, 2B; *Corollary* 2 *to Lemma* 4A);

(ii) *every two elements of G generate a group; three elements generate a group if and only if they are associative in some order* (*Theorem* 2A);

(iii) *the associator A of G is a characteristic normal subloop of G* (*Theorem* 3B);

(iv) *a necessary and sufficient condition that the inner mapping group* $\mathfrak{J}$ *be a group of automorphisms of* G *is that* G/A *be a commutative Moufang loop in which every element save the identity has order* 3 ((iii) *above and Corollary* 1 *to Theorem* 4B);

(v) *the set* C *consisting of all elements commutative with the elements of* G *is a characteristic commutative subloop of* G, *the Moufang centre. If* u, v *are in* C, $R_{u,v}$ *is an automorphism of* G (*Corollary* 1 *to Theorem* 4C; *Theorem* 4B).

THEOREM 7B. *If* G *is a commmutative Moufang loop, then*:

(i) G *is characterized by the law* $x^2 \cdot yz = xy \cdot xz$ (*a consequence of Theorem* 4C);

(ii) *every two elements of* G *generate an abelian group*; *every three generate an abelian group if and only if they are associative in some order* (*Theorem* 2A);

(iii) *the mapping* $x \rightarrow x^3$ *is an endomorphism of* G *into its centre* Z (*Corollary* 2 *to Theorem* 4B);

(iv) *the inner mapping group of* G *is a group of automorphisms*; *hence every characteristic subloop of* G *is normal in* G (*Corollary* 2 *to Theorem* 4B).

By use of Theorem 7B we may readily extend our knowledge of commutative Moufang loops.

THEOREM 7C([15]). *If* G *is a commutative Moufang loop, then*:

(i) *the subset* F *of* G, *consisting of all elements of finite order, is a characteristic* (*hence normal*) *subloop of* G;

(ii) F *is a direct product* $F = A \times N$ *where* A *is a subgroup of the centre* Z *of* G *and where* N *contains every element of* G *of order a power of* 3; *moreover* A *and* N *are characteristic* (*normal*) *subloops of* F *and of* G;

(iii) N *contains the derived loop* G'; *in fact* $x^3 = 1$ *for every element of* G';

(iv) G/F *is an abelian group.*

Proof. (i) If x, y are in F, every element of the abelian group $\{x, y\}$ has finite order. Hence F is a subloop of G. The rest follows by Theorem 7B (iv).

(ii) Let A consist of all elements of F of order prime to 3. Then A is a characteristic, hence normal, subloop of G, by the above argument. In view of Theorem 7B (iii), $A \leqq Z$. Similarly N is a characteristic normal subloop of G. If the element x of F is neither in A nor in N then, since $\{x\}$ is a finite abelian group, x has a unique representation $x = yz$ with y in A, z in N. Since $A \cap N = 1$ by construction, the proof is complete.

(iii) G' is generated by the set of all elements $x^{-1} \cdot xS$ with x in G, S in the inner mapping group $\mathfrak{J}$ of G. By (iii), (iv) of Theorem 7B, $(x^{-1} \cdot xS)^3 = x^{-3} \cdot (xS)^3 = x^{-3} \cdot (x^3)S = x^{-3} \cdot x^3 = 1$. Hence $y^3 = 1$ for every element y of G'.

(iv) This follows since $F \geqq N \geqq G'$.

Again, if T is the kernel of the homomorphism $x \rightarrow x^3$, G/T is isomorphic

[15] It seems apparent from Bol's paper [1] that he was at least partly aware of the truth of Theorem 7C. However, no such theorem is stated in his paper.

to a subgroup of the centre Z. We may state this as a corollary.

COROLLARY TO THEOREM 7C. *Let T be the subset of N consisting of all elements x of G such that $x^3=1$. Then $T \geqq G'$ is a characteristic (normal) subloop of G, and G/T is isomorphic to a subgroup of Z.*

Clearly the corollary could have been used to prove (iii).

THEOREM 7D. *Let G be a commutative Moufang loop with associated group $\mathfrak{G} = \{R_x; x \in G\}$. Then:*

(i) *the inner mapping group $\mathfrak{J}$ of G is contained in the derived group $\mathfrak{G}' = (\mathfrak{G}, \mathfrak{G})$ of $\mathfrak{G}$;*

(ii) *a necessary and sufficient condition that G be centrally nilpotent of class $c \leqq 2$ is that the group $\mathfrak{G}$ possess an endomorphism $X \rightarrow X^3$ into its centre (and thus incidentally be nilpotent of class at most 3);*

(iii) *if G is centrally nilpotent of class 2, $\mathfrak{G}$ is nilpotent of class 3. Then, by* (i), (ii), *$\mathfrak{J}$ is a commutative group of automorphisms of G, each of order 3.*

Proof. (i) Since G is commutative we may use the defining relation $x^2 \cdot yz = xy \cdot xz$ along with $L_x = R_x$. By (ii) of Theorem 7B it follows that

$$R_x^n = R_{x^n} \tag{7.1}$$

for every integer n, positive, negative or zero. Thus the defining relation yields $L_y L_x{}^2 = L_x L_y$ or

$$R_{xy} = R_x^{-1} R_y R_x^2. \tag{7.2}$$

From (1) by interchange of x and y we have $R_{x,y} = R_x R_y R_{xy}{}^{-1} = R_x R_y R_y{}^{-2} R_x{}^{-1} R_y = R_x R_y{}^{-1} R_x{}^{-1} R_{xy}$ or

$$R_{x,y} = (R_x^{-1}, R_y). \tag{7.3}$$

Thus each $R_{x.y}$ is in $(\mathfrak{G}, \mathfrak{G})$, and since these generate the inner mapping group $\mathfrak{J}$ of the commutative loop G, the result follows.

(ii) First suppose that the loop G is centrally nilpotent of class $c \leqq 2$, and let S be in $\mathfrak{J}$, x in G. Then the element $\alpha = x^{-1} \cdot xS$ is in $Z \cap G'$. Since α is in G', $\alpha^3 = 1$ by (iii) of Theorem 7C, and since α is in Z, $\alpha S = \alpha$. But $xS = \alpha x$, $xS^2 = (\alpha x)S = \alpha S \cdot xS = \alpha.\ \alpha x = \alpha^2 x$, and $xS^3 = (\alpha^2 x)S = \alpha^2 \cdot \alpha x = \alpha^3 \cdot x = x$. Thus $S^3 = I$ for every S of $\mathfrak{J}$. Again, if y is in G, $yR_x S = (yx)S = yS \cdot xS = yS \cdot \alpha x = (y\alpha)S \cdot x = yR_\alpha S R_x$ and so $R_x S = R_\alpha S R_x$. Furthermore, since α is in the centre of G, R_α is in the centre of $\mathfrak{G}$. Now $(SR_x)^2 = SR_x SR_x = S(R_\alpha S R_x) R_x = R_\alpha S^2 R_x{}^2$, and $(SR_x)^3 = R_\alpha S^2 R_x{}^2 S R_x = R_\alpha{}^3 S^3 R_x{}^3 = R_\alpha{}^3 R_x{}^3 = R_x{}^3$. But x^3 is in the centre of G and so $(SR_x)^3 = R_x{}^3$ is in the centre of $\mathfrak{G}$. Since every element of G has the form SR_x with S in $\mathfrak{J}$, x in G, it follows that the cube of every element of $\mathfrak{G}$ is in the centre of $\mathfrak{G}$. If T is also in $\mathfrak{J}$, and if $xT = \beta x$, then, by the same reasoning, $(SR_x)(TR_y) = R_\beta STR_x R_y = R_\beta U R_{xy}$, where $U = STR_{x,y}$ is in $\mathfrak{J}$, and so $(SR_x \cdot TR_y)^3 = R_\beta{}^3 R_{xy}{}^3 = R_x{}^3 R_y{}^3 = R_x{}^3 R_y{}^3 = (SR_x)^3 (SR_x)^3$. Hence the mapping $X \rightarrow X^3$, for X in $\mathfrak{G}$, is an endomorphism of $\mathfrak{G}$ into its centre.

Now let us assume that $\mathfrak{G}$ possesses an endomorphism $X \rightarrow X^3$ into its centre. By Theorem 1A, $\mathfrak{G}' = (\mathfrak{G}, \mathfrak{G})$ is an abelian group, and by (i) of the present theorem, $\mathfrak{G}' \geqq \mathfrak{I}$. Thus if $\mathfrak{I}_1$ is the normalizer of $\mathfrak{I}$ in $\mathfrak{G}$, $\mathfrak{I}_1 \geqq \mathfrak{G}'$. Hence $\mathfrak{I}_1$ is a normal subgroup of G, and so $\mathfrak{I}_2 = \mathfrak{G}$ where $\mathfrak{I}_2$ is the normalizer of $\mathfrak{I}_1$ in $\mathfrak{G}$. A reference to Theorem 8B of Chapter I reveals that G is centrally nilpotent of class at most 2, the case of class 2 arising only when $\mathfrak{I}_1 \neq \mathfrak{G}$.

(iii) If G is an abelian group, $\mathfrak{G}$ is an isomorphic group, and hence $\mathfrak{G}$ has class 0 or 1 according as G contains exactly one element or more than one element. Conversely if $\mathfrak{G}$ is an abelian group, so is G. We now must show that if G is centrally nilpotent of class 2, $\mathfrak{G}$ cannot have class 2. Suppose on the contrary that $\mathfrak{G}$ has class 2. Then $\mathfrak{I}$, as a subgroup of $\mathfrak{G}'$, is contained in the centre of $\mathfrak{G}$, and hence is a normal subgroup of $\mathfrak{G}$. This is impossible, since then, in the notation of the last paragraph, we would have $\mathfrak{I}_1 = \mathfrak{G}$, in contradiction to the fact that G has class 2. Since the only remaining possibility is that $\mathfrak{G}$ have class 3, the proof is complete.

8. **Construction of commutative Moufang loops.** We first give a simplified version of a result previously announced by the author (Bruck [1, §9]).

THEOREM 8A. *Let G be an I.P. loop and let the loop G_o be a principal isotope of G given by*

$$xoy = xf \cdot gy \tag{8.1}$$

where f, g are fixed elements of G. Then a necessary and sufficient condition that G_o have the inverse property is that f, g be Moufang elements of G.

COROLLARY 1. *Every loop isotopic to a Moufang loop is Moufang.*

Proof. It should be noted that every principal loop-isotope of an I.P. loop can be obtained in the form (8.1). Since moreover every isotope of a loop is isomorphic to a principal isotope, the corollary follows immediately from Theorem 8A. Now consider the equation

$$zo(xoy) = y, \tag{8.2}$$

which, by use of (8.1), can be written successively in the following equivalent forms: $(zf)[g(xf \cdot gy)] = y$, $g(xf \cdot gy) = (zf)^{-1} \cdot y$, and

$$(zf)^{-1} = [g(xf \cdot gy)] \cdot y^{-1}. \tag{8.3}$$

We may say that G_o has the *left* inverse property if for each x the solution z of (8.2) is independent of y. Hence a necessary and sufficient condition that G_o have the left inverse property is that the right-hand side of (8.3) be independent of y. Now if g is a Moufang element, (L_g, R_g, L_gR_g) and thus (L_gR_g, L_g^{-1}, L_g) are autotopisms of G. In this case $g(xf \cdot gy) = (xf \cdot gy)L_g = [(xf)L_gR_g][(gy)L_g^{-1}] = [(g \cdot xf)g]y$, and hence (8.3) can be written as

$$(8.4) \qquad (zf)^{-1} = (g\cdot xf)g,$$

which shows that z is independent of y. Conversely, if z is independent of y, we equate the right-hand side of (6.3) to its expression for $y=1$; thus $[g(xf\cdot gy)]y^{-1}=g(xf\cdot g)$, or $g(xf\cdot gy)=[g(xf\cdot g)](g^{-1}\cdot gy)$, whence (R_gL_g, L_g^{-1}, L_g) is an autotopism, and g a Moufang element, of G.

In similar fashion the equation

$$(8.5) \qquad (yox)oz = y$$

may be replaced by the equivalent equation

$$(8.6) \qquad (gz)^{-1} = y^{-1}[(yf\cdot gx)f].$$

If f is a Moufang element of G, (L_f, R_f, L_fR_f) and (R_f^{-1}, L_fR_f, R_f) are autotopisms of G; by virtue of the latter autotopism (6.6) may be replaced by

$$(8.7) \qquad (gz)^{-1} = (f\cdot gx)f,$$

whence z is independent of y, G_0 has the right inverse property. Conversely, if we equate the right-hand side of (8.6) to its value for $y=1$, we derive $(yf\cdot gx)f=(yf\cdot f^{-1})[(f\cdot gx)f]$, whence (R_f^{-1}, L_fR_f, R_f) is an autotopism, and f a Moufang element, of G.

From (8.4), (8.7) we get formally distinct expressions for the inverse z of x in G_0. That these are the same may be verified either by computations with elements or by reference to Theorem 2B. With this the proof is complete. From what has gone before the truth of the following corollary is evident.

COROLLARY 2. *A necessary and sufficient condition that the loop G_0 given by* (8.1) *have the left inverse property* (*right inverse property*) *is that $g(f)$ be a Moufang element of the I.P. loop G.*

In preparation for further study it will be convenient to have a theorem on arbitrary loops.

THEOREM 8B. *Let G be a loop with unit* 1, *and let G_o be the principal isotope of G defined by*

$$(8.8) \qquad xoy = xR_b^{-1}\cdot yL_a^{-1},$$

with unit $e=ab$. If the mapping S yields an endomorphism of G into its centre, then the mapping T, defined by

$$(8.9) \qquad xT = xS\cdot(eS)^{-1}\cdot e,$$

yields an endomorphism of G_o into the centre of G_0.

Proof. It follows from the work of §§1, 2 of Chapter I (cf. the proof of Theorem 1D, Chapter I) that the mapping

$$(8.10) \qquad x\rightarrow xe$$

induces an isomorphism of the centre of G upon the centre of G_0. Hence, since S is an endomorphism of G into its centre, it follows that xT is in the centre of G_0 for all x of G_0. Now $(xoy)S=(xSR_{bS}^{-1})(ySL_{aS}^{-1})=(xS)(bS)^{-1}(yS)(aS)^{-1}$ $=(xS)(yS)[(ab)S]^{-1}=(xS)(yS)(eS)^{-1}$, and so

$$(8.11) \qquad (xoy)T = (xS)(yS)(eS)^{-2}e.$$

On the other hand, by the above remark in connection with (8.10), $(ue)o(ve)$ $=uve$ for any two elements u, v of the centre of G. Hence in particular

$$(8.12) \qquad (xT)o(yT) = (xS)(eS)^{-1}(yS)(eS)^{-1}e = (xS)(yS)(eS)^{-2}e.$$

From (8.11) and (8.12) it follows that $(xoy)T=(xT)o(yT)$ for all x, y of G_0, and thus that the mapping T yields an endomorphism of G_0 into its centre.

One remark is perhaps in order. In (8.9) and in the derivation of (8.11) we introduced inverses, for example the element $(aS)^{-1}$. This was permissible, for arbitrary loops, in view of the fact that the elements in question lay in the centre of the loop.

THEOREM 8C. *Let G be a Moufang loop with the property that the mapping $x\rightarrow x^3$ is an endomorphism of G into its centre. Then a like property holds for every loop isotopic to G.*

Proof. It is clearly necessary to treat only the case of the principal isotope G_0 given by (8.1). If h be defined by

$$(8.13) \qquad h = fg,$$

then G_0 has unit $e=h^{-1}$. Thus, by virtue of Theorem 8B, it is sufficient to prove that

$$(8.14) \qquad xoxox = xT \equiv x^3(h^{-1})^{-3}h^{-1} = x^3h^2.$$

(Note that we have omitted parentheses in (8.14), since G_0, like G, is a Moufang loop.) Now, by (8.1), $xox = xf\cdot gx = (x\cdot fg)x = xh\cdot x = xhx$, and so $(xox)ox = [(xhx)f](gx) = [x\cdot(h\cdot xf)]\cdot(f^{-1}h\cdot x) = x\cdot[(h\cdot xf)\cdot f^{-1}h]\cdot x$ $=x\cdot[h\cdot(xf\cdot f^{-1})h]x=xhxhx=(xh)^3h^{-1}=x^3h^3h^{-1}=x^3h^2$. Thus (8.14) is verified. (In this computation we have made several uses of formula (2.5) and one use of the formula $(xhx)f=x\cdot(h\cdot xf)$, which latter amounts to employing the autotopism (L_xR_x, L_x^{-1}, L_x).)

It is well known that all the isotopes of a commutative loop G are commutative if and only if G is an abelian group. Since there exist non-associative commutative Moufang loops, the following corollary is not without interest. For proof we cite Theorems 7B (iii), 8C.

COROLLARY TO THEOREM 8C. *Every loop H isotopic to a commutative Moufang loop has the property that the mapping $x\rightarrow x^3$ is an endomorphism of H into its centre.*

THEOREM 8D. *If the mapping $x \rightarrow x^3$ is an endomorphism of the Moufang loop G into its centre, the groupoid G_0 defined by*

$$xoy = x^{-1}yx^2 \tag{8.15}$$

is a commutative Moufang loop. Moreover:

(i) *if H is a subloop of G the set H_o, consisting of the same elements as H, is a subloop of G,*

(ii) *if H is a normal subloop of G, H_0 is a normal subloop of G_0, and G_0/H_0 is isomorphic to the loop $(G/H)_0$ formed from G/H by the method of* (8.15);

(iii) *if H is in the centre of G, H_0 is in the centre of G_0.*

Proof. First we verify that G_0 is commutative. Now $(xoy)(yox)^{-1} = x^{-1}yx^2(y^{-1}xy^2)^{-1} = x^{-1}yx^2y^{-2}x^{-1}y = x^3y^{-3} \cdot x^{-1}yx^{-1}yx^{-1}y = x^3y^{-3}(x^{-1}y)^3 = x^3 \cdot x^{-3}y^3 \cdot y^{-3} = 1$, hence $xoy = yox$. Next, by Theorem 7B(i), we must show that

$$(xoy)o(xoz) = (xox)o(yoz) \tag{8.16}$$

for all x, y, z of G_0. From (8.15) it is clear that

$$xox = x^2, \qquad (xoy)^3 = x^3y^3. \tag{8.17}$$

The left-hand side of (8.16) may be written as

$$\begin{aligned}(xoy)^{-1}(xoz)(xoy)^{-1}(xoy)^3 &= (x^{-2}y^{-1}x)(x^{-1}zx^2)(x^{-2}y^{-1}x)x^3y^3 \\ &= (xy^{-1}x)(x^{-1}zx^{-1})(xy^{-1}x)y^3 \\ &= (xy^{-1}x \cdot x^{-1})(zx^{-1} \cdot xy^{-1}x)y^3 \\ &= (xy^{-1})\left\{\left[(zx^{-1} \cdot x)y^{-1}\right]x\right\}y^3 \\ &= (xy^{-1})(zy^{-1} \cdot x)y^3 = x(y^{-1}zy^{-1})x \cdot y^3 \\ &= x(y^{-1}zy^2)x = x(yoz)x,\end{aligned}$$

and thus we have

$$(xoy)o(xoz) = x(yoz)x. \tag{8.18}$$

Again, $(xox)o(yoz) = x^2o(yoz) = x^{-2}(yoz)x^4 = x^{-2}(yoz)xx^3 = x(yoz)x$, and so

$$(xox)o(yoz) = x(yoz)x. \tag{8.19}$$

But (8.18) and (81.9) together imply (8.18). Thus G_0 is a commutative Moufang loop.

We now proceed to the remaining assertions of Theorem 8D.

(i) This is obvious.

(ii) From (8.15) and the fact that G_0 is commutative we see that the right and left mappings of G_0 are given by

$$\overset{0}{R}_x = \overset{0}{L}_x = \overset{2}{R}_x \overset{-1}{L}_x. \tag{8.20}$$

Since G_0 and G have the same unit 1, it follows that the inner mapping group of G_0 is contained in that of G. Thus, by (i) and this fact, H_0 is a normal subloop of G_0 when H is a normal subloop of G. Moreover, by (8.15) and the normality of H in G, we readily derive the equations

$$xoH = xH, \qquad (xH)o(yH) = (xoy)H, \tag{8.21}$$

which imply, first, that the cosets of H_0 in G_0 are identical with those of H in G, and, secondly, that $(G/H)_0$ is isomorphic to G_0/H_0.

(iii) This follows from the above remark on inner mapping groups, and the fact that centre elements are self-conjugate.

We now specialize the situation of Theorem 8D by taking the Moufang loop G to be associative.

THEOREM 8E. *Let G be a group with centre Z, derived group G'; and let C be the centralizer*[16] *of G' in G. Further let the mapping $x\rightarrow x^3$ be an endomorphism of G into Z. Then, if G_0 is the commutative Moufang loop obtained from G via* (8.15):

(i) *C_0 is the centre of G_0;*

(ii) *G_0 is centrally nilpotent of class $c\leqq 2$, equality holding if and only if the nilpotent group G has class* 3;

(iii) *if G has class* 3, *and if $H=(G', G)$, then H_0 is the centrally derived loop of G_0;*

(iv) *the inner mapping group $\mathfrak{J}_0$ of G_0 is isomorphic to the abelian group $G'/(G'\cap Z)$.*

Proof. First let us consider the equation

$$(cox)oy = do(xoy). \tag{8.22}$$

By (8.15), $(cox)oy=yo(xoc)=y^{-1}x^{-1}cx^2y^2$, and $do(xoy)=(xoy)od=(xoy)^{-1}d(xoy)^2$. Thus (8.22) is equivalent to $y^{-1}x^{-1}cx^2y^2=(xoy)^{-1}d(xoy)^2$ or to

$$d(xoy)^2y^{-2}x^{-2} = (xoy)y^{-1}x^{-1}c. \tag{8.23}$$

But (8.22) is satisfied for all x, y when $c=d=1$. Hence, from (8.23), $(xoy)^2y^{-2}x^{-2} = (xoy)y^{-1}x^{-1} = x^{-1}yx^2y^{-1}x^{-1}=(y^{-1}x)^{-1}x^2(y^{-1}x)x^{-2}=(y^{-1}x, x^{-2})$ $=(y^{-1}x, x)$, the last equation holding since x^3 is in Z. Thus (8.22) or (8.23) is equivalent to $d(y^{-1}x, x)=(y^{-1}x, x)c$ or to

$$d = (x, y^{-1}x)^{-1}c(x, y^{-1}x). \tag{8.24}$$

We now consider in turn the various items of Theorem 8E.

(i) The element c is in the centre of G_0 if and only if (8.22) is satisfied, with $d=c$, for all x, y of G. Thus (8.24) must hold with $d=c$ for all x, y, and it follows that $ac=ca$ for every element a of G'. Thus c is in C. Conversely if c is in C, (8.24), and hence (8.22), is satisfied, with $d=c$, for all x, y of G.

[16] The centraliser (in G) of the subset S of the group G is the subgroup of G consisting of all elements of G which commute with every element of S.

Thus the Moufang loop C_0, derived from C via (8.15), is the centre of G_0.

(ii) By Theorem 1A, G' is an abelian group. Hence $C \geqq G'$, and G_0/C_0 is an abelian group isomorphic to G/C. Thus G_0 has central class $c \leqq 2$. Now $C=G$ if and only if $G' \leqq Z$, and hence G_0 is an abelian group if and only if G has class less than 3. In other words, G_0 has class 2 if and only if G has class 3.

(iii) If G has class 3, G/H has class 2 and hence G_0/H_0 is abelian, $H_0 \geqq K_0$, where K_0 is the centrally derived loop of G_0. But K_0, as a subgroup of $Z_0 \equiv Z$, is identical with a subgroup K of Z. Thus K is a normal subgroup of G, and since G_0/K_0 is abelian, G/K must have class at most 2. Hence $K \geqq H \geqq K$, whence $K=H$. This completes the proof of (iii).

(iv) From the fact that (8.22) is equivalent to (8.24) we see that $\mathfrak{J}_0$ is isomorphic to the group of mappings $c \rightarrow a^{-1}ca$ of G into itself, where a ranges over all elements of G'. Hence G' is homomorphic to $\mathfrak{J}_0$, the kernel of the homomorphism being $G' \cap Z$.

THEOREM 8F. *Let H be a commutative Moufang loop, centrally nilpotent of class at most* 2. *Further let $G=\{R_x; x \in H\}$ be the group associated with H, and let $K \leqq G'$ be the inner mapping group of H. Then*:

(i) *H is isomorphic to a subloop of the commutative Moufang loop G_0 obtained from G via* (8.15);

(ii) *K_0 is a normal subloop of G_0*;

(iii) *H is isomorphic to G_0/K_0.*

COROLLARY. *Every commutative Moufang loop which is centrally nilpotent of class at most 2 is among the subloops of (and the homomorphs of) the loops G_0 obtained by the method of Theorem* 8E.

Proof. (i) That G_0 is a commutative Moufang loop (centrally nilpotent of class at most 2) follows from Theorems 7D (ii) and 8E. Now the elements R_x, R_y of G are in G_0 and, moreover, by (8.15), (7.2), $R_x o R_y \equiv R_x^{-1}R_yR_x^2=R_{xy}$. Hence the one-to-one mapping $x \rightarrow R_x$ yields an isomorphism of H into G_0. This proves (i).

(ii) By Theorem 7D (i), K is a subgroup of G' and hence K_0 is a subloop of G_0'. Since G' is commutative, by Theorem 1A, G' lies in its centraliser C, and so $K_0 \leqq G_0' \leqq C_0$. But C_0 is the centre of G_0, by Theorem 8E (i), and hence K_0, as a subloop of C_0, is a normal subloop of G_0.

(iii) The elements of G_0/K_0 have the form K_0oR_x, x in G. Moreover $(K_0oR_x)o(K_0oR_y)=K_0o(R_xoR_y)=K_0oR_{xy}$, by (i), and hence the mapping $x \rightarrow K_0oR_x$ is a homomorphism of H upon G_0/K_0. The kernel of this homomorphism is the set of elements x such that $K_0oR_x=K_0$, or that R_x is in K. But R_x is in K if and only if $1R_x=x=1$. This completes the proof of (iii).

The corollary is of course an immediate consequence of Theorem 8F. It is interesting to note that if in this corollary the phrase "method of Theorem 8E" be replaced by "method of Theorem 8D" the statement becomes wholly trivial. Indeed the commutative Moufang loops are among those which possess an endomorphism $x \to x^3$ into the centre, and if the G of Theorem 8D is commutative, the corresponding G_0 is identical with G. However every isotope G of commutative Moufang loop H possesses an endomorphism $x \to x^3$ into its centre (Theorem 8C) and yet not every such G is commutative; so that it seems worthwhile to consider the properties of the corresponding G_0. As we shall now see, nothing new results.

THEOREM 8G. *If G is an isotope of the commutative Moufang loop H, and if G_0 is the commutative Moufang loop obtained from G via* (8.15), *then G_0 is isomorphic to H.*

Proof. We shall let xy designate the product of x and y in H and assume (as we may without loss of generality) that G is the principal isotope H_* of H given by

$$x * y = xf \cdot gy, \tag{8.25}$$

where f, g are fixed elements of H. A reference to Theorem 8A shows that the inverse of x in G is the element z given by (8.3) or (8.4). Using (8.4), we see that

$$zf = g^{-1}(f^{-1}x^{-1})g^{-1} = g^{-2}(f^{-1}x^{-1}). \tag{8.26}$$

Again (8.15), when interpreted in the present circumstances, gives

$$xoy = z * [y * (x * x)]. \tag{8.27}$$

It will also be convenient to set $fg = e^{-1}$, so that e is the unit of G and G_0, and

$$fg = e^{-1}, \qquad g^{-1} = ef = fe. \tag{8.28}$$

Now $x * x = xf \cdot gx = x \cdot fg \cdot x = xe^{-1}x = e^{-1}x^2$, and $g(x * x) = (e^{-1}f^{-1})(e^{-1}x^2) = e^{-2}(f^{-1}x^2)$. Thus $u \equiv y * (x * x) = (yf)[g(x * x)] = (fy)(f^{-1}x^2 \cdot e^{-2}) = f^2[y\{f^{-1}(f^{-1}x^2 \cdot e^{-2})\}]$ $= f^{-1}[y\{f^2(f^{-1}x^2 \cdot e^{-2})\}] = f^{-1}[y\{x^2 \cdot fe^{-2}\}]$, or

$$u \equiv y * (x * x) = f^{-1}[y(x^2 \cdot fe^{-2})]. \tag{8.29}$$

But $xoy = z * u = (zf)(gu) = [g^{-2}(f^{-1}x^{-1})](gu) = g^{-3} \cdot g^2[f^{-1}x^{-1} \cdot u]$, or

$$xoy = z * u = (ef)(f^{-1}x^{-1} \cdot u). \tag{8.30}$$

Next, from (8.29), $f^{-1}x^{-1} \cdot u = f^{-2}\{x^{-1}[y(x^2 \cdot fe^{-2})]\} = f^{-2}\{x^2[y(x^{-1} \cdot fe^{-2})]\}$ $= f^{-2}[(xy)(fe^{-2})] = (f^{-1} \cdot xy)e^{-2} = (ef)^{-1}(e^{-1} \cdot xy)$, and so by (8.30),

$$xoy = e^{-1} \cdot xy. \tag{8.31}$$

It follows from (8.31) that the mapping $x \to ex$ is an isomorphism of H upon G_0; in fact $(ex)o(ey) = e^{-1}(ex \cdot ey) = e^{-1}(e^2 \cdot xy) = e \cdot xy$. This completes the proof of Theorem 8G.

In the next theorem we consider a special case of the extension problem for commutative Moufang loops.

THEOREM 8H. *Let M be a Moufang loop with unit* 1, *which possesses an endomorphism $x \rightarrow x^3$ into its centre. Let E be the cyclic group of order* 3, *written additively, with elements* 0, 1, 2, *and let $G=(M, E)$ be the set of all couples (x, p) with x in M, p in E, where $(x, p)=(y, q)$ if and only if $x=y$, $p=q$. Finally let multiplication in G be defined by*

$$(8.32) \qquad (x, p)(y, q) = (\phi_{q-p}(x, y), p + q)$$

where

$$(8.33) \qquad \phi_0(x, y) = x^{-1}yx^2, \qquad \phi_1(x, y) = xy, \qquad \phi_2(x, y) = yx,$$

for all x, y of M and p, q of E. Then:

(i) *G is a commutative Moufang loop*[17];

(ii) *M is isomorphic to a subloop of a loop isotopic to G;*

(iii) *$G=M\times E$ if and only if M is commutative;*

(iv) *if M is not commutative, the centre of G consists of all elements (x, o) with x in the centre of M;*

(v) *if N is a normal subloop of M, the set of all elements (x, o) with x in N is a normal subloop H of G, isomorphic to N, and G/H is isomorphic to the loop $(M/N, E)$ obtained from M/N as G is obtained from M;*

(vi) *a necessary and sufficient condition that G be centrally nilpotent of class c is that M be centrally nilpotent of class c.*

COROLLARY 1. *Every Moufang loop which possesses an endomorphism $x \rightarrow x^3$ into its centre is either an isotope of a commutative Moufang loop or a normal subloop of index 3 in such an isotope. (But there exist loops of this type which are isotopic to no commutative Moufang loop, namely the noncommutative groups.)*

COROLLARY 2. *There exists a commutative Moufang loop which is centrally nilpotent of class* 3.

Proof. (i) It follows from (8.33) and from Theorem 8D that, for each fixed p of E, $\phi_p(x, y)$ defines the product of x and y in a quasigroup (which is in fact a Moufang loop). Thus, by the general extension theory for loops (Albert [2], Bruck [2, §10]) G is a loop. According to Theorem 7B(i), G is a commutative Moufang loop if and only if $(x, p)^2[(y, q)(z, r)] = [(x, p)(y, q)][(x, p)(z, r)]$, or, equivalently, if and only if

$$(8.34) \qquad \phi_{u+v}[\phi_0(x, x), \phi_{v-u}(y, z)] = \phi_{v-u}[\phi_u(x, y), \phi_v(x, z)].$$

(In (8.34) we have set $u=q-p$, $v=r-p$; and it is to be understood that this equation must hold for all x, y, z of M and u, v of E.) The truth of (8.34) in the case $u=v=0$ is a consequence of Theorem 8D. There remain eight cases, which we must consider in detail. In the cases $u=v=1$ and $u=v=2$, (8.34) becomes respectively

[17] In §9 we shall show that every commutative Moufang loop G with a cyclic quotient loop E may be constructed essentially as in Theorem 8H.

$$(8.35)\qquad (y^{-1}zy^2)x^2 = (xy)^{-1}(xz)(xy)^2$$

and

$$(8.36)\qquad x^2(y^{-1}zy^2) = (yx)^{-1}(zx)(zx)^2.$$

But since M is Moufang, $(y^{-1}zy^{-1})x^{-1}=y^{-1}(z\cdot y^{-1}x^{-1})=[(xy)^{-1}\cdot x][z(xy)^{-1}]=(xy)^{-1}(xz)(xy)^{-1}$, and so $(y^{-1}zy^2)x^2=[(y^{-1}zy^{-1})x^{-1}](xy)^3=(xy)^{-1}(xz)(xy)^2$. Thus (8.35) is true, and by taking inverses we get $x^{-2}(y^{-2}zy^{-1})=(y^{-1}x^{-1})^2\cdot(z^{-1}x^{-1})(y^{-1}x^{-1})^{-1}$, which, since u^3 is in the centre for every u, is equivalent to (8.36). This completes the cases in which $v=u$. When $v=u+1$, (8.34) becomes $\phi_{1-u}(x^2, yz)=\phi_u(x, y)\phi_{1+u}(x, z)$; and, taking $u=0, 1, 2$ in turn, we get

$$(8.37)\qquad x^2\cdot yz = (x^{-1}yx^2)(xz),$$

$$(8.38)\qquad x^{-2}(yz)x^4 = xy\cdot zx,$$

$$(8.39)\qquad (yz)x^2 = (yx)(x^{-1}zx^2).$$

Now (8.37), on division by x^3, becomes $x^{-1}\cdot yz=(x^{-1}yx^{-1})(xz)$, which is true since $(L_x^{-1}R_x^{-1}, L_x, L_x^{-1})$ is an autotopism of M; and (8.39) comes from (8.37) by taking inverses. The left-hand side of (8.38) is equal to $x(yz)x=xy\cdot zx$. Finally, when $v=u+2$, (8.34) becomes $\phi_{2-u}(x^2, zy)=\phi_{2+u}(x, z)\phi_u(x, y)$. But interchange of y and z and replacement of u by $u+1$ gives exactly the equation corresponding to $v=u+1$. This completes the proof of (i).

(ii) Since $(x, p)(1, 1)=(\phi_{1-p}(x, 1), p+1)=(x, p+1)$ and, similarly, $(1, 2)(y, q)=(y, 2+q)$, it follows that the loop G_0 with multiplication

$$(8.40)\qquad (x, p)o(y, q) = (x, p+1)(y, 2+q) = (\phi_{q-p+1}(x, y), p+q)$$

is isotopic to G. Moreover the set H of elements of form (x, o) is a normal subloop of G_0. But $(x, o)o(y, o)=(xy, o)$, and so H is isomorphic to M under the mapping $(x, o)\rightarrow x$.

(iii) If M is commutative it is evident that $G=M\times E$, and this is impossible otherwise, since G is commutative.

(iv) A necessary and sufficient condition that the element (x, p) be in the centre of G is that $[(x, p)(y, q)](z, r)=(x, p)[(y, q)(z, r)]$ for all y, z of M, q, r of E. If u, v are defined by $u=r-q$, $v=q-p$, this condition reduces to

$$(8.41)\qquad \phi_{u+p}[\phi_v(x, y), z] = \phi_{u-p}[x, \phi_u(y, z)],$$

holding for all y, z of M and u, v of E. But the right-hand side of (8.41) is independent of v, and thus (8.41) may be replaced by the two equations

$$(8.42)\qquad \phi_v(x, y) = \phi_1(x, y) = xy,$$

$$(8.43)\qquad \phi_{u+p}(xy, z) = x\phi_u(y, z).$$

Now (8.42) with $v=2$ yields $yx=xy$, whence x *must commute with every element of* M. But then $\phi_0(x, y)=x^{-1}yx^2=xy$, and so (8.42) yields nothing more. If

$(x, 1)$ is in the centre of G, then $(x, 1)(x^{-1}, 2)=(\phi_1(x, x^{-1}), 0)=(1, 0)$, and so $(x^{-1}, 2)$ is also in the centre. Thus we need only consider (8.43) in the cases $p=0$, $p=1$.

The case $p=0$. Then (8.43) becomes $\phi_u(xy, z)=x\phi_u(y, z)$. From this with $u=1$ we get $xy\cdot z=x\cdot yz$, whence x must not only commute with every element of M, but also lie in the associator of M. This means that x is in the centre of M. But, conversely, every centre element clearly satisfies (8.41) for $p=0$, as we see from (8.33).

The case $p=1$. From (8.43) with $u=0$ we get

$$(8.44) \qquad xy\cdot z = x(y^{-1}zy^2).$$

Since interchange of y and z leaves the right-hand side of (8.44) invariant, we have in particular

$$(8.45) \qquad xy\cdot z = xz\cdot y.$$

From (8.44) with z replaced by yz we obtain $xy\cdot yz=x\cdot zy^2$. We use without comment (8.45) and the fact that x commutes with M to get, successively, $x\cdot zy^2=xy\cdot yz=yx\cdot yz=yxy\cdot z=xy^2\cdot z=xz\cdot y^2$. Thus $x\cdot zy^2=xz\cdot y^2$ or $x\cdot zy^{-1}=xz\cdot y^{-1}$ for all z, y, whence, as before, x is in the centre of M. But then (8.45) yields $yz=zy$, in contradiction to the fact that M is not commutative. Hence the centre of G contains no elements of form $(x, 1)$ or $(x, 2)$. This completes the proof of (iv).

(v) It is immediately evident from (8.33) and the normality of N that $\phi_p(Nx, y)=N\phi_p(x, y)$ for all x, y of G. Thus if $H=(N, o)$, $H(x, p)=(Nx, p)$, $[H(x, p)](y, q)=(N\phi_{q-p}(x, y), p+q)$ and $\{[H(x, p)](y, q)\}\{(x, p)(y, q)\}^{-1}=(N, o)=H$. Hence H is mapped into itself by every generator of the inner mapping group, and so is a normal subloop of G. To see that G/H is isomorphic to $(M/N, E)$ we note that $H(x, p)=(Nx, p)$ and that $[H(x, p)][H(y, q)]=(\phi_{q-p}(Nx, Ny), p+q)$.

(vi) If G is centrally nilpotent of class c, so is every loop-isotope of G, and thus M, as a subloop of an isotope of G, is centrally nilpotent of class $d\leqq c$. But conversely, if M is centrally nilpotent of class d, it follows from (iii), (iv) and (v) that G is centrally nilpotent of class $c\leqq d$. Thus we have $c\leqq d\leqq c$, whence $c=d$.

The first statement of Corollary 1 is a consequence of (ii) and of Theorem 8C. As to the second statement, every loop-isotope of a group is an isomorphic group. Corollary 2 follows from (vi) and Theorem 1B.

It is still an open question as to whether every Moufang loop which possesses an endomorphism $x\rightarrow x^3$ into its centre is centrally nilpotent. In view of (vi) and of Corollary 1, this need only be proved for commutative loops.

9. **The derived loop of a commutative Moufang loop.** If G is a commutative I.P. loop we have $L_x=R_x$ for all x of G. Moreover, since $R_{x,y}=R_xR_yR_{xy}^{-1}$,

it follows that $R_{x,y}{}^{-1} = R_{xy}R_{y^{-1}}R_x{}^{-1} = R_{xy,y^{-1}}$. Thus, by §§3, 7 of Chapter I we see that *the (centrally) derived loop G' of G is generated by the set of all triples*

$$(9.1) \qquad [x, y, z] \equiv x^{-1}\cdot xR_{y,z} = x^{-1}\{(xy\cdot z)(yz)^{-1}\}$$

with x, y, z in G. In what follows we shall assume that the commutative loop G is Moufang.

Lemma 9A. *Let G be a commutative Moufang loop with center Z, derived loop G', so that G' is generated by the set of all triples $[x, y, z]$ defined by* (9.1). *Then*:

(i) $xy\cdot z = (x[x, y, z])(yz)$;
(ii) *if c is in Z*, $[cx, y, z] = [x, cy, z] = [x, y, cz] = [x, y, z]$;
(iii) $[x, y, z]^3 = 1$;
(iv) $[x, y, z]^{-1} = [y, x, z]$;
(v) $[x, y, z] = [y, z, x]$;
(vi) *if p, q, r are rational integers*, $[x^p, y^q, z^r] = [x, y, z]^{pqr}$;
(vii) $[x, y, z] = [x, y, yz]$.

Remark. From (iv) and (v) it follows that interchange of any two of x, y, z in the triple $[x, y, z]$ replaces the triple by its inverse. Thus, by this and (iii), if two of x, y, z are equal, $[x, y, z] = 1$. Hence the triple behaves very much like a three-index skew-symmetric tensor. The analogy would be even more evident if G were written additively.

Proof. (i) and (ii) should be obvious, and (iii) follows from the fact that the mapping $x \to x^3$ is an endomorphism of G into Z. In further stages of the proof it will be convenient to have the formula

$$(9.2) \qquad x^{-1}\cdot yz = x^{-3}(xy\cdot xz).$$

In fact, since x^3 is in Z, $x^{-1}\cdot yz = x^{-3}(x^2\cdot yz) = x^{-3}(xy\cdot xz)$, by the defining relation for commutative Moufang loops. We also use without further comment the fact that every two elements of G generate a group.

If $A_y \equiv (R_y, R_y, R_y{}^2)$, then A_y is an autotopism of the commutative Moufang loop G, and hence so is $A_yA_zA_{yz}{}^{-1} = (R_{y,z}, R_{y,z}, R_{y^2,z^2})$. It follows at once that $R_{y,z} = R_{y^2,z^2}$, and hence that $[x, y, z] = [x, y^2, z^2]$. But $y^2 = y^3\cdot y^{-1}$, and y^3 is in Z. Thus, by (ii),

$$(9.3) \qquad [x, y, z] = [x, y^{-1}, z^{-1}].$$

Again, by two uses of (9.2), $[x, y, z] \equiv x^{-1}\{(xy\cdot z)(y^{-1}z^{-1})\} = x^{-3}\{x(xy\cdot z)\}\cdot\{x\cdot y^{-1}z^{-1}\} = (y\cdot x^{-1}z)(x\cdot y^{-1}z^{-1})$, whence

$$(9.4) \qquad [x, y, z] = (x\cdot y^{-1}z^{-1})(y\cdot x^{-1}z) = [y, x, z^{-1}].$$

Next we have $[x, y, yz] \equiv x^{-1}\{(xy\cdot yz)(y\cdot yz)^{-1}\} = x^{-1}\{(xz\cdot y^2)(zy^2)^{-1}\} = [x, z, y^2] = [x, z, y^3y^{-1}] = [x, z, y^{-1}]$, whence by (9.4),

$$(9.5) \qquad [x, y, yz] = [z, x, y].$$

Similarly, by (9.2), $[x, y, y^{-1}z] \equiv x^{-1}\{(xy\cdot y^{-1}z)(y\cdot y^{-1}z)^{-1}\} = x^{-1}\{(xy\cdot y^{-1}z)z^{-1}\} = x^{-1}\{(xy\cdot z)(y^{-1}z\cdot z)\}z^{-3} = x^{-1}\{(xy\cdot z)(y^{-1}z^{-1})\} = [x, y, z]$, so

$$[x, y, y^{-1}z] = [x, y, z]. \tag{9.6}$$

In (9.6) we replace z by yz and use (9.5), deriving

$$[x, y, z] = [z, x, y]. \tag{9.7}$$

It follows from (9.7) that $[x, y, z]$ is invariant under cyclic permutations of x, y, z. Thus (9.7) is equivalent to (v). Moreover (9.5) and (9.7) together imply (vii). Since the mapping $x\rightarrow x^{-1}$ is an automorphism of G we see that

$$[x, y, z]^{-1} = [x^{-1}, y^{-1}, z^{-1}]. \tag{9.8}$$

From (9.8), (9.3), (v) and (9.4) we have $[x, y, z]^{-1} = [x^{-1}, y^{-1}, z^{-1}] = [x^{-1}, y, z] = [y, z, x^{-1}] = [z, y, x] = [y, x, z]$, which proves (iv). As to (vi), it is clear from (ii), (iii) that proof need only be given when p, q, r are prime to 3. Indeed, by (iv), there is no loss of generality in assuming $p=1$. The case $q=r=1$ is trivial; the case $q=r=-1$ follows from (9.3); moreover $[x, y, z^{-1}] = [y, x, z] = [x, y, z]^{-1}$ and so $[x, y^{-1}, z] = [z, x, y^{-1}] = [z, x, y]^{-1} = [x, y, z]^{-1}$. This completes the proof of Lemma 9A.

As a next step in the study of the generators of G' it is natural to consider the five-fold symbol $[[u, v, w], x, y]$. In view of the "skew-symmetry" of the triple $[x, y, z]$, one might wonder whether the relation

$$[[u, v, w], x, y] = [[y, u, v], w, x] \tag{9.9}$$

held for every G. We shall now show that this is not the case.

Lemma 9B. *A necessary and sufficient condition that* (9.9) *be true for all* u, v, w, x, y *of the commutative Moufang loop G is that G be centrally nilpotent of class at most* 2.

Corollary. *There exist commutative Moufang loops G in which* (9.9) *is violated.*

Proof. *Sufficiency.* It follows from (9.9) that the five-fold symbol $F = [[u, v, w], x, y]$ is invariant under cyclic permutation of u, v, w, x, y. Thus, by Lemma 9A, F is "skew-symmetric" in its five arguments; in particular $F=1$ whenever two arguments are equal. Since $R_{x,y}$ is an automorphism of G, we have $(pq)R_{x,y} = p'q'$, where we have written $p' = pR_{x,y}$, $q' = qR_{x,y}$ for convenience. By this fact, by Lemma 9A(i), and by the "skew-symmetry" of F, we have $(pq)[pq, x, y] = (pq)R_{x,y} = pR_{x,y}\cdot q' = (p[p, x, y])q' = ([p, x, y]p)q' = ([p, x, y][[p, x, y], p, q'])(pq') = [p, x, y](pq')$. But similarly $pq' = p\{q[q, x, y]\} = ([q, x, y]q)p = [q, x, y](qp)$, and so $(pq)[pq, x, y] = \{(pq)\cdot[q, x, y]\}[p, x, y] = \{(pq)[pq, [q, x, y], [p, x, y]]\}\{[q, x, y][p, x, y]\}$. As we shall show in a moment,

$$[z, [q, x, y], [p, x, y]] = 1 \tag{9.10}$$

and so $(pq)[pq, x, y] = (pq)\{[q, x, y][p, x, y]\}$ or

$$[pq, x, y] = [p, x, y][q, x, y] \tag{9.11}$$

for all p, q, x, y of G. As to (9.10), if $w = [q, x, y]$, then $[z, w, [p, x, y]] = [[p, x, y], z, w] = [[w, p, x], y, z]$ by (9.9); but $[w, p, x] = [[q, x, y], p, x] = 1$ by skew-symmetry. Hence (9.10) follows from Lemma 9A(ii). It is clear from (9.11) that, for each fixed pair x, y of G, the mapping $p \rightarrow [p, x, y]$ is an endomorphism of G. Thus in particular $[[u, v, w], x, y] = [[u, x, y], [v, x, y], [w, x, y]] = 1$, by (9.10). It follows that each triple $[u, v, w]$ lies in Z. Hence $G' \leqq Z$, G is centrally nilpotent of class at most 2.

Necessity. If $G' \leqq Z$, $[[u, v, w], x, y] = 1$ for all u, v, w, x, y and hence (9.9) is trivially satisfied.

The corollary follows from Lemma 9B and Theorem 8H, Corollary 2. We have proved incidentally that (9.11) holds when $G' \leqq Z$. The following lemma generalizes this result.

LEMMA 9C. *Let G be a commutative Moufang loop with centre Z, and let Z_2/Z be the centre of G/Z. Then* (9.11) *holds for every x in Z_2 and for all p, q, y of G.*

Proof. If x is in Z_2, $[p, x, y]$ is in Z for all p, y of G. Thus $(pq)[pq, x, y] = (pq)R_{x,y} = pR_{x,y} \cdot qR_{x,y} = (p[p, x, y])(q[q, x, y]) = (pq)[p, x, y][q, x, y]$; and so (9.11) is verified. Note that if G is centrally nilpotent of class at most 2, $Z_2 = G$.

LEMMA 9D. *If G is a commutative Moufang loop,*

$$xz^p \cdot yz^q = \{(xy)[x, y, z]^{p-q}\}z^{p+q} \tag{9.12}$$

for all x, y, z of G and for all rational integers p, q.

Proof. In proving (9.12) we may assume the integers p, q to be reduced modulo 3. When $q = p$, the equation is trivially verified. Again, if it is true for a certain pair p, q, it is true for the pair q, p, as we see by interchanging x and y. Therefore we may assume $p = 1$. First we take $q = -1$. Now $(xz \cdot yz^{-1})^{-1} = x^{-1}z^{-1} \cdot y^{-1}z = (xy)^2\{(x^{-1}y^{-1} \cdot x^{-1}z^{-1})(x^{-1}y^{-1} \cdot y^{-1}z)\} = (xy)^2 \{(x^{-2} \cdot y^{-1}z^{-1})(y^{-2} \cdot x^{-1}z)\} = x^{-3}y^{-3}(xy)^2\{(x \cdot y^{-1}z^{-1})(y \cdot x^{-1}z)\} = (x^{-1}y^{-1})[x, y, z]$ by (9.4), and hence (9.12) is true in this case. Next take $q = 0$. But $(xz \cdot y)z^{-1} = (xz^2 \cdot yz)z^{-3} = (xz^{-1} \cdot yz) = (yx)[y, x, z]^{-1} = (xy)[x, y, z]$ by the case $p = 1$, $q = -1$, and so $xz \cdot y = \{(xy)\ [x, y, z]\}z$. This concludes the proof.

We are now ready to consider the problem of constructing Moufang loops with a given number of generators.

THEOREM 9A. *Let $n \geqq 3$ be a fixed integer, and let G be the set of all couples $A = (a_i, a_{ijk})$ where a_i is an n-dimensional tensor with rational integral coeffi-*

cients and where a_{ijk} is an n-dimensional skew-symmetric tensor with rational integral coefficients reduced modulo 3. *Define the product* $AB=P$ *by*

$$(9.13)\qquad p_i = a_i + b_i \qquad (i = 1, 2, \cdots, n),$$

$$(9.14)\qquad p_{ijk} \equiv a_{ijk} + b_{ijk} + (a_ib_j - a_jb_i)(a_k - b_k) \pmod 3,$$

where in (9.14) *it is assumed that* $1 \leqq i \leqq j \leqq k \leqq n$. *Then*:

(i) *G is a commutative Moufang loop*;

(ii) *the centre Z of G consists of all elements A of G such that* $a_i \equiv 0 \pmod 3$ *for* $i=1, 2, \cdots, n$;

(iii) *the derived loop G' of G consists of all elements A of G such that* $a_i=0$ *for* $i=1, 2, \cdots, n$;

(iv) *G is centrally nilpotent of class* 2;

(v) *if K is the complement of G' in the centre $Z=G'\times K$, G/K has order 3^α, where* $\alpha=C_{n,1}+C_{n,3}$;

(vi) *a necessary and sufficient condition that a commutative Moufang loop H with n generators be centrally nilpotent of class* 2 *is that H be a homomorphic image of G.*

Proof. (i) It is evident from the definition that AB is uniquely defined and that $AB=BA$ for all A, B of G. Moreover if $U=(0, 0)$ we see that $UA=AU=A$ for all A, so that U is the unit element of G. If P, A are given, we may solve uniquely for B from the equation $AB=P$; in fact $b_i=p_i-a_i$, by (9.13), and hence (for $1\leqq i\leqq j\leqq k\leqq n$) $b_{ijk}\equiv p_{ijk}-a_{ijk}+(a_ip_j-a_jp_i)(a_k+p_k) \pmod 3$, by (9.14). In particular, when $P=U$, we have $b_i=-a_i$, $b_{ijk}\equiv -a_{ijk} \pmod 3$, and hence are led to define

$$(9.15)\qquad A^{-1} = (-a_i, \ -a_{ijk}).$$

By direct substitution we see that $AB=P$ implies $B=A^{-1}P$. Thus G is a commutative I.P. loop.

It is convenient to define the *sum* of A and B:

$$(9.16)\qquad A + B = (a_i + b_i, a_{ijk} + b_{ijk}).$$

If further we define $f(a, b)$ to be the element $(a_i, o)(b_i, o)$, so that

$$(9.17)\qquad f(a, b) = (0, r_{ijk}), \quad r_{ijk} \equiv (a_ib_j - a_jb_i)(a_k - b_k) \pmod 3,$$

we see that

$$(9.18)\qquad AB = A + B + f(a, b).$$

We shall also make use of the elements of form

$$(9.19)\qquad [a, b, c] = (0, t_{ijk}), \ t_{i,j,k} \equiv \begin{vmatrix} a_i & a_j & a_k \\ b_i & b_j & b_k \\ c_i & c_j & c_k \end{vmatrix} \pmod 3.$$

It is a consequence of (9.16) and (9.18) that $A^2=AA=2A$. Hence

$$A^2\cdot BC = 2A + B + C + f(b, c) + f(-a, b+c)$$

while on the other hand

$$AB\cdot AC = 2A + B + C + f(a, b) + f(a, c) + f(a+b, a+c),$$

where for example a and $a+b$ denote respectively the tensors a_i and a_i+b_i. Thus a necessary and sufficient condition that G be a commutative Moufang loop is that, for all tensors a, b, c,

$$(9.20)\qquad f(b, c) + f(-a, b+c) = f(a, b) + f(a, c) + f(a+b, a+c).$$

But, for $1\leqq i\leqq j\leqq k\leqq n$, the ijk component of the right-hand side of (9.20) is

$$\begin{vmatrix} a_i & a_j \\ b_i & b_j \end{vmatrix}(a_k-b_k) + \begin{vmatrix} a_i & a_j \\ c_i & c_j \end{vmatrix}(a_k-b_k) + \begin{vmatrix} a_i+b_i, & a_j+b_j \\ a_i+c_i, & a_j+c_j \end{vmatrix}(b_k-c_k),$$

which may easily be rearranged as

$$\begin{vmatrix} b_i & b_j \\ c_i & c_j \end{vmatrix}(b_k-c_k) + \begin{vmatrix} a_i & a_j \\ b_i+c_i, & b_j+c_j \end{vmatrix}(a_k+b_k+c_k),$$

the corresponding component of the left-hand side. This completes the proof of (i).

(ii) *and* (iii). We now wish to derive the formula

$$(9.21)\qquad (AB\cdot C)(BC)^{-1} = A + [a, b, c],$$

where $[a, b, c]$ is given by (9.19). Direct substitution gives $(AB\cdot C)(BC)^{-1} -A =f(a, b)-f(b, c)+f(a+b, c)+f(a+b+c, -b-c)$. But the ijk component of the latter is congruent (mod 3) to

$$\begin{vmatrix} a_i & a_j \\ b_i & b_j \end{vmatrix}(a_k-b_k) - \begin{vmatrix} b_i & b_j \\ c_i & c_j \end{vmatrix}(b_k-c_k)$$
$$+\begin{vmatrix} a_i+b_i & a_j+b_j \\ c_i & c_j \end{vmatrix}(a_k+b_k-c_k)$$
$$+\begin{vmatrix} a_i+b_i+c_i & a_j+b_j+c_j \\ -b_i-c_i & -b_j-c_j \end{vmatrix}(a_k-b_k-c_k) \equiv \begin{vmatrix} a_i & a_j & a_k \\ b_i & b_j & b_k \\ c_i & c_j & c_k \end{vmatrix},$$

as may be verified by a straightforward calculation.

Again, after multiplying (9.21) on both sides by $A^{-1}=-A$, we see that

$$(9.22)\qquad [A, B, C] = [a, b, c]$$

where the triple on the left is defined as in (9.1). Thus it follows that $A=(a, a_{ijk})$ is in Z if and only if $[a, b, c]=U$ for all b, c. Clearly $[a, b, c]=U$

when $a_i \equiv 0 \pmod 3$ for all i. But conversely, if for fixed $i<j<k$ we choose b, c so that $b_j=1$, $c_k=1$ but all other components of b, c are zero we find that the ijk component of $[a, b, c]$ is congruent to a_i mod 3; whence $[a, b, c]=U$ implies $a_i \equiv 0 \pmod 3$. This completes the proof of (ii).

As for (iii), it is clear from (9.22) that if $A \in G'$ then $a_i=0$ for $i=1, 2, \cdots, n$. Conversely we may show that a, b, c may be chosen so that $[a, b, c]=(0, t_{i,j,k})$ has $t_{i,j,k} \equiv 0 \pmod 3$ except when i, j, k are permutations of three arbitrarily chosen indices $u<v<w$, and hence that G' contains every element A of G whose component a is zero. Thus (iii) is proved. Incidentally we may note at the same time that G has exactly n generators, namely the vectors a with one component equal to 1 and the others equal to 0.

(iv) This is an immediate consequence of (ii) and (iii).

(v) Since G' is a subgroup of the abelian group Z it follows that Z is a direct product $Z=G'\times K$, where in fact K consists of those elements $A=(a, a_{i,j,k})$ such that $a_i \equiv 0 \equiv a_{ijk} \pmod 3$ for all i, j, k. K, as a subgroup of the centre Z of B, is a normal subloop of G; and G/K may be represented as the set of couples $A=(a_i, a_{ijk})$ where the tensors a_i and a_{ijk} have components in $GF(3)$, and where multiplication is defined as before. The number of distinct tensors a_i and a_{ijk} are thus 3^n and 3^m, where $m=C_{n,3}$. From these remarks (v) follows at once.

(vi) Let H be a commutative Moufang loop, centrally nilpotent of class 2, written multiplicatively. Let $g_1, g_2, \cdots, g_n$ be a set of generators of H, independent in the sense that no subset of these elements will generate H. Since H has class 2, the triples $[g_i, g_j, g_k]$ are in the centre of H. Moreover, in view of the "skew-symmetry" of these triples (see Lemma 9A), we shall use as (integral) exponents only skew-symmetric tensors a_{ijk}. Moreover the a_{ijk}, by Lemma 9A (iii), may be reduced modulo 3. If a_i is a tensor with rational integral components we define the elements A_i of H recursively by

$$A_1 = g_1^{a_1}, \qquad A_i = A_{i-1}\cdot g_i^{a_i} \qquad \text{for } 1 < i \leqq n. \tag{9.23}$$

Finally we set

$$A = \prod_{i<j<k} [g_i, g_j, g_k]^{a_{ijk}}\cdot A_n. \tag{9.24}$$

If B is similarly defined, corresponding to tensors b_i and b_{ijk}, and P, corresponding to tensors p_i and p_{ijk}, we wish to show that $AB=P$ where P is determined by (9.13) and (9.14). Before proving this point it will be well to note its implications. First we shall have that the set of all elements of type (9.24) is a loop, which therefore must coincide with H. Secondly, since, as will be seen, we shall raise no questions as to the identity of two elements of type (9.24), it will be clear that H is a homomorphic image of G.

Because of the complications of notation we merely sketch the proof, which is fairly straightforward. By Lemma 9D and the fact that the triples

$[x, y, z]$ are in the centre,

$$(9.25)\quad A_nB_n = (A_{n-1}\cdot g_n^{a_n})(B_{n-1}\cdot g_n^{b_n}) = [A_{n-1}, B_{n-1}, g_n]^{a_n-b_n}\cdot(A_{n-1}B_{n-1})\cdot g_n^{a_n+b_n}.$$

From (9.23), (9.24) and (9.25) we see by mathematical induction that $AB \equiv P \pmod{G'}$, where we may take $p_i = a_i + b_i$, $i = 1, 2, \cdots, n$. Thus it is only necessary to determine the p_{ijk}. Since the mapping $x \to [x, y, g_n]$ is, for each fixed y, an endomorphism of H into its centre, we may verify that

$$(9.26)\qquad [A_{n-1}, B_{n-1}, g_n] = \prod_{i<j<n} [g_i, g_j, g_n]^{c(i,j)}$$

where $c(i, j) \equiv a_ib_j - a_jb_i \pmod 3$. Thus from (9.23), (9.24) and (9.25) we see that, for $i<j<n$, we may take $p_{ijn} \equiv a_{ijn} + b_{ijn} + (a_ib_j - a_jb_i)(a_n - b_n) \pmod 3$. The rest of the proof follows by induction.

Remarks. (i) *When $n = 3$, the loop G/K of order 3^4, considered in Theorem* 9A(v), *is abstractly identical with that constructed by Bol* [1].

(ii) *It is easily deduced from* (9.21) *that the inner mapping group of the loop G constructed in Theorem* 9A *is isomorphic with G'; that is, with an abelian group of type* (1^m), *order 3^m, where $m = C_{n,3}$.*

We shall conclude this section by pointing out the intimate connection between Theorem 8H and Lemma 9D. Let G be a commutative Moufang loop and let H be a normal subloop of G such that G/H is a cyclic group. If f is a representative of G/H in G the elements of G all have the form xf^p where p is an integer and x is in H. According to Lemma 9D we have

$$(9.27)\qquad xf^p\cdot yf^q = \{(xy)[x, y, f]^{p-q}\}f^{p+q},$$

where of course $[x, y, f]$ is in H whenever x and y are. If we set

$$(9.28)\qquad \phi_p(x, y) = (xy)[x, y]^p$$

where $[x, y] = [x, f, y]$ we note first that $\phi_p(x, y) = \phi_q(x, y)$ for all x, y of H whenever $p \equiv q \pmod 3$. Now the loop G_0, isotopic to G, defined by

$$(9.29)\qquad (xf^p)o(yf^q) = (xf^p\cdot f)\cdot(yf^q\cdot f^{-1}) = \phi_{q-p+1}(x, y)f^{p+q},$$

has as subloop H_0 consisting of the same elements as H under the multiplication

$$(9.30)\qquad xoy = \phi_1(x, y) = (xy)[x, y].$$

In view of Theorem 8C, H_0 is a Moufang loop such that the mapping $x \to xoxox$ is an endomorphism into its centre, and, in view of Theorem 8H, every Moufang loop with this property can be obtained in the same manner as H_0.

Upon these remarks may be based several observations. First it should be seen that Theorem 8H may be generalized by replacing the 3-group E of that theorem by the additive group of integers and by insisting that ϕ_p and ϕ_q coincide whenever $p \equiv q \pmod 3$. Secondly it would seem that, given somewhat more knowledge than we have at our disposal at present, it should be possible, by use of (9.28), to treat the extension problem discussed in the last paragraph in terms of the loop H alone, without use of the non-commutative loop M introduced in Theorem 8H.

The crux of the matter seems to be the determination of a complete but simple set of characteristic properties of the binary operation $[x, y]$ of HH on H. Note that $[x, y]=[x, f, y]$, so that $[x, y]$ must have the known properties of a triple; but, among other things, f is not an element of H. In the following theorem, the proof of which we omit, we impose upon $[x, y]$ conditions which are sufficient for the purpose, but which hardly seem necessary.

THEOREM 9B. *If H is a commutative Moufang loop, if $[x, y]$ is a binary operation on HH to H, and if H_0 is the set consisting of the same elements of H, with product xoy defined by* (9.30), *then the following postulates ensure that H_0 is a Moufang loop. Moreover, when the postulates hold, the mapping $x \rightarrow xoxox$ is an endomorphism of H_0 into its centre*:

For all x, y, z of H, (i) $[x, x]=1$; (ii) $[y, x]=[x, y]^{-1}$; (iii) $[[x, y], z] =[[y, z], x]$; (iv) *for every fixed v of the subloop $\{x, y, z\}$, the mapping $u \rightarrow [u, v]$ (and hence, by* (ii), *the mapping $u \rightarrow [v, u]$) induces an endomorphism of $\{x, y, z\}$ into its centre.*

In regard to the proof we merely remark that it can be shown, on the basis of (i), (ii), (iii) and (iv), that $x^{-1}o(xoy)=(yox)ox^{-1}=y$ and that $(xoy)o(zox) =\{xo(yoz)\}ox=x^2\cdot yz$. (Note that all operations are actually performed within the subloop $\{x, y, z\}$.) If H has centre Z and H/Z has centre Z_2/Z, we may satisfy the postulates by setting $[x, y]=[x, y, h]$ where h is any fixed element of Z_2 (see Lemma 9C), with the slight difference that the mapping $x \rightarrow [x, y]$ will then be an endomorphism of H into its centre.

Theorem 9B generalizes an earlier construction of the author [1, §5], as is especially apparent when H is written additively and $[x, y]$ is regarded as a product operation on H.

10. **The inner mapping group of a Moufang loop.** In §3 we derived necessary and sufficient conditions that the inner mapping group $\mathfrak{J}$ of a Moufang loop G be a group of automorphisms of G (Theorem 4B and corollaries). In particular this is true when G is commutative. We now wish to subject the inner mapping group to a closer study. For a Moufang loop G we may use equations (4.7) or

$$(10.1)\qquad L_{yx}=R_y^{-1}L_xR_yL_y, \qquad R_{xy}=L_y^{-1}R_xL_yR_y,$$

together with (4.9) or

$$(10.2)\qquad L_xR_x=R_xL_x.$$

The groups $\mathfrak{G}_\lambda=\{L_x; x \text{ in } G\}$, $\mathfrak{G}_\rho=\{R_x; x \text{ in } G\}$ and the group $\mathfrak{G}=\{\mathfrak{G}_\lambda, \mathfrak{G}_\rho\}$ *associated* with G will play an important part. By the corollary to Lemma 4D,

$\mathfrak{G}_\lambda$, $\mathfrak{G}_\rho$ are normal subgroups of $\mathfrak{G}$, and hence so are $\mathfrak{G}_\lambda\cap\mathfrak{G}_\rho$ and $(\mathfrak{G}_\lambda, \mathfrak{G}_\rho)$, their intersection and their commutator group respectively.

Now $\mathfrak{J}$ is generated by the set of all permutations

$$(10.3) \qquad L_{x,y} = L_xL_yL_{yx}^{-1}, \qquad R_{x,y} = R_xR_yR_{xy}^{-1}, \qquad T_x = R_xL_x^{-1}.$$

But from (10.1), $L_{x,y}=L_xL_y\cdot L_y^{-1}R_y^{-1}L_x^{-1}R_y=L_xR_y^{-1}L_x^{-1}R_y=(L_x^{-1}, R_y)$, and similarly $R_{x,y}=R_xL_y^{-1}R_x^{-1}L_y=(R_x^{-1}, L_y)$, whence

$$(10.4) \qquad L_{x,y} = (L_x^{-1}, R_y), \qquad R_{x,y} = (R_x^{-1}, L_y), \qquad L_{x,y} = R_{y^{-1},x^{-1}}^{-1}.$$

Thus, in particular, *the set of all $L_{x,y}$ generates the same subgroup of $\mathfrak{J}$ as does the set of all $R_{x,y}$*. This subgroup we shall designate by $\mathfrak{K}$.

It is readily deduced from the proof of Theorem 3B of Chapter I that the set of all $R_{x,y}$ generates that subgroup of $\mathfrak{G}_\rho$ consisting of all U in $\mathfrak{G}_\rho$ such that $1U=1$. Thus $\mathfrak{K}=\mathfrak{J}\cap\mathfrak{G}_\rho$, and by further arguments of the same sort we obtain the following lemma.

LEMMA 10A. *If G is a Moufang loop, then, in the above notation, $\mathfrak{J}\cap\mathfrak{G}_\lambda=\mathfrak{J}\cap\mathfrak{G}_\rho=\mathfrak{J}\cap(\mathfrak{G}_\lambda\cap\mathfrak{G}_\rho)=\mathfrak{K}$. Moreover $\mathfrak{K}$, together with the set of all T_x, generates $\mathfrak{J}$.*

COROLLARY. *If G is a commutative Moufang loop, $\mathfrak{J}\leqq(\mathfrak{G}, \mathfrak{G})=\mathfrak{G}'$.*

LEMMA 10B. *If G is a Moufang loop, the permutation*

$$(10.5) \qquad U_{x,y} = T_xT_yT_{xy}^{-1}$$

is in $\mathfrak{K}$ for all x, y of G.

Proof. By Lemma 10A, it will be sufficient to show that $U_{x,y}$ is in $\mathfrak{G}_\lambda$, since it clearly is in $\mathfrak{J}$. But $\mathfrak{G}_\lambda$ is a normal subgroup of $\mathfrak{G}$, and so, from the definition of T_x, $U_{x,y}=R_xL_x^{-1}R_yL_y^{-1}L_{xy}R_{xy}^{-1}\in R_xR_yR_{xy}^{-1}\mathfrak{G}_\lambda=R_{x,y}\mathfrak{G}_\lambda\leqq\mathfrak{K}\mathfrak{G}_\lambda=\mathfrak{G}_\lambda$.

THEOREM 10A. *If G is a Moufang loop, then, in the notation of this section, $\mathfrak{K}$ is a normal subgroup of $\mathfrak{J}$, and the mapping $x\rightarrow\mathfrak{K}T_x$ is a homomorphism of G upon the group $\mathfrak{J}/\mathfrak{K}$. The kernel of this homomorphism is $N=1[\mathfrak{G}_\lambda\cap\mathfrak{G}_\rho]$; that is, the set of all elements $1P$ with P in $\mathfrak{G}_\lambda\cap\mathfrak{G}_\rho$.*

COROLLARY. *The inner automorphism group of a group G is isomorphic to the central quotient group G/Z.*

Proof. Since $\mathfrak{G}_\lambda$ is normal in $\mathfrak{G}$, then $\mathfrak{K}=\mathfrak{J}\cap\mathfrak{G}_\lambda$ is normal in $\mathfrak{J}$. By Lemma 10B, $\mathfrak{K}T_xT_yT_{xy}^{-1}=\mathfrak{K}$, and so

$$(10.6) \qquad (\mathfrak{K}T_x)\cdot(\mathfrak{K}T_y) = \mathfrak{K}T_{xy}.$$

Since $\mathfrak{K}$ and the T_x generate $\mathfrak{J}$, and since G has the inverse property, (10.6) completes the proof of the first assertion. The kernel of the homomorphism clearly consists of those x for which T_x is in $\mathfrak{K}$, or for which $T_x=R_xL_x^{-1}=U$ with U in $\mathfrak{K}$. But then $R_x=UL_x$, whence R_x is in $\mathfrak{K}\mathfrak{G}_\lambda=\mathfrak{G}_\lambda$, or R_x is in $\mathfrak{G}_\lambda\cap\mathfrak{G}_\rho$. Conversely, every element of $\mathfrak{G}_\lambda$ has form UL_x with U in $\mathfrak{K}$, every element of $\mathfrak{G}_\rho$ has form VR_y with V in $\mathfrak{K}$, and $UL_x=VR_y$ implies $x=1\,UL_x=1\,VR_y=y$. In this case, $UL_x=VR_x$, $T_x=V^{-1}U\in\mathfrak{K}$. Thus $N=1\,[\mathfrak{G}_\lambda\cap\mathfrak{G}_\rho]$, as stated. The corollary follows from the fact that, on the one hand, $\mathfrak{K}\leqq(\mathfrak{G}_\lambda,\mathfrak{G}_\rho)=I$, while, on the other hand, $T_x\in\mathfrak{K}=I$ if and only if $R_x=L_x$, x is in Z. It is thus apparent that Theorem 10A gives a direct generalization of a familiar theorem on groups.

Note that if G is commutative the homomorphism $x\rightarrow\mathfrak{K}T_x$ becomes trivial, since $T_x=I$ for all x. It will be convenient to make the following definition.

Definition. The Moufang loop G is a Moufang loop of the first kind if $\mathfrak{G}_\lambda=\mathfrak{G}_\rho=\mathfrak{G}$; otherwise G is of the second kind.

Lemma 10C. *A necessary and sufficient condition that the Moufang loop G be of the first kind is that the homomorphism considered in Theorem* 10A *be trivial.*

Proof. *Necessity.* If $\mathfrak{G}_\lambda=\mathfrak{G}_\rho=\mathfrak{G}$ then $\mathfrak{G}_\lambda\cap\mathfrak{G}_\rho=\mathfrak{G}$ and so $N=1\mathfrak{G}=G$. Thus, by Theorem 9A, the homomorphism $x\rightarrow\mathfrak{K}T_x$ is trivial.

Sufficiency. If $T_x=R_xL_x^{-1}$ is in $\mathfrak{K}\leqq\mathfrak{G}_\lambda\cap\mathfrak{G}_\rho$ for all x, then $R_x\in\mathfrak{K}L_x\leqq\mathfrak{G}_\lambda$. Hence $\mathfrak{G}_\rho\leqq\mathfrak{G}_\lambda$, and similarly $\mathfrak{G}_\lambda\leqq\mathfrak{G}_\rho$, so that $\mathfrak{G}_\lambda=\mathfrak{G}_\rho=\mathfrak{G}$.

It is readily verified that every loop-isotope of a Moufang loop of the first kind is also a Moufang loop of the first kind. And hence a like statement is true for Moufang loops of the second kind.

Theorem 10B. *If G is a Moufang loop of the second kind, and if the descending chain condition holds for subloops of G, there exists an integer $n\geqq 1$ and a strictly decreasing series*

$$G=H_0>H_1>\cdots>H_n \tag{10.7}$$

of subloops of G with the following properties:

(i) *for each $j=1,2,\cdots,n$, H_j is the associatrally derived loop of H_{j-1}, and incidentally H_{j-1}/H_j is a group;*

(ii) *the associatrally derived loop of H_n is H_n;*

(iii) *H_n is a Moufang loop of the first kind.*

Remark. It follows from Theorem 10B, in particular, that every finite Moufang loop may be built up from a Moufang loop of the first kind by successive extensions by groups.

Proof. By definition, the associatrally derived loop H_1 of a loop G is the intersection of all normal subloops K of G such that G/K is a group. Thus (§3), H_1 is a normal subloop of G and G/H_1 is a group. For $j>1$ we define H_j as in (i). If, for some integer j, $H_j=H_{j+1}$, it is clear that $H_j=H_k$ for every integer $k\geqq j$. In view of the descending chain condition, such a j exists; the smallest such j we call n. Thus (ii) is verified. As to (iii), assume, if possible, that the Moufang loop H_n is of the second kind. In this case, as we see from Lemma 10C, there exists a proper normal subloop N of H_n such that H_n/N is a group. But then $H_n > N \geqq H_{n+1}$, in contradiction to (ii). Hence H_n is of the first kind.

Theorem 10C. *The associator of a Moufang loop G of the first kind coincides with the centre.*

Proof. The associator A of G consists of all elements a of G such that $a\mathfrak{K}=a$, as follows from Theorem 3A and the present section. But since G is of the first kind, $\mathfrak{K}=\mathfrak{J}$, by Lemma 10C, and hence A coincides with the centre of G.

Theorem 10D. *If G is a finite Moufang loop of order g, and if G is associatrally nilpotent, the order of the associated group* $\mathfrak{G}$ *divides some power of g.*

Corollary. *A finite Moufang p-loop is associatrally nilpotent if and only if it is centrally nilpotent.*

Proof. As before let $\mathfrak{J}=\mathfrak{J}(G)$ be the inner mapping group of G, and let $\mathfrak{K}=\mathfrak{K}(G)$ be the normal subgroup of $\mathfrak{J}$ generated by the set of all $R_{x,y}$ with x, y in G. Then, by Theorem 10A, $\mathfrak{J}/\mathfrak{K}$ is a homomorphic image of G, and hence the order of $\mathfrak{J}/\mathfrak{K}$ divides g. We shall now show that the order of $\mathfrak{K}$ divides some power of g. This part of the proof follows closely the proofs of Lemmas 8A, 8B, and Theorem 8A of Chapter I, and hence a brief sketch should be sufficient. The mapping $U \rightarrow U'$, where U' is defined by

$$(xA)U' = (xU)A \tag{10.8}$$

for all x of G, and where A is the associator of G, yields a homomorphism of $\mathfrak{K}(G)$ upon $\mathfrak{K}(G/A)$, the kernel of the homomorphism being the set $\mathfrak{L}$ of all U of $\mathfrak{K}$ such that $xU \in xA$ for all x of G. We assume inductively that the order of $\mathfrak{K}/\mathfrak{L}$ divides some power of the order of G/A, and hence some power of g. Now $a\mathfrak{K}=a$ for every a of A. Hence if U is in $\mathfrak{L}$, so that for each fixed x of G we have $xU \in xA = Ax$, or $xU = ux$ for u in A, then $(xa)U = xU \cdot aT = ux \cdot a = u \cdot xa$, since $T = L_x U L_{xU}^{-1}$ is in $\mathfrak{J} \cap \mathfrak{G}_\lambda = \mathfrak{K}$. Thus the element u is uniquely determined by U and the coset xA. Again $x = (xU)U^{-1} = (ux)U^{-1} = u \cdot xU^{-1}$, and so $xU^{-1} = u^{-1}x$. Finally, if V is in $\mathfrak{L}$, and if $xV = vx$, then $xUV = (ux)V = u \cdot vx = uv \cdot x$. Hence, for each fixed coset xA, the mapping $U \rightarrow u = xUR_x^{-1}$ is a homomorphism of $\mathfrak{L}$ into A. If we designate by θ the union of these homomorphisms, the kernel of θ is the identity mapping, for if $U\theta = 1$ then $xU = x$ for all x of G, whence $U = I$. It follows that $\mathfrak{L}$ is isomorphic to a subgroup of a (finite) direct power of A. Hence the order of $\mathfrak{L}$ divides some power of g. Thus, in view of our inductive assumption, the order of $\mathfrak{K}$, and hence the order of $\mathfrak{J}$, divides some power of g. Finally, by Corollary 4 to Theorem 3B, Chapter I, the order of the associated group $\mathfrak{G}$ divides some power of g.

As for the Corollary to Theorem 10D, if the associatrally nilpotent Moufang loop G is a finite p-loop, the associated group $\mathfrak{G}$ is a p-group and hence (Theorem 8C of Chapter I) G is centrally nilpotent. It is of course trivially evident that every centrally nilpotent loop is associatrally nilpotent.

Chapter III. Special theory. Examples and constructions

Here again, all references to theorems and sections refer to Chapter III, unless the contrary is explicitly stated.

Our main concern in Chapter III is to study in greater detail the various entities introduced in Chapters I and II. This we do in various ways, sometimes considering quite general problems of construction, as in §§2 and 3, and at other times tackling more special problems which nonetheless involve situations of considerable generality, as in §§1, 5, 6, 7. In contrast with these we have §4, which deals with one specific counterexample.

In §1 we consider the construction of the most general loop E which contains as a normal subloop a given abelian group G, such that E/G is a given abelian group H. Thus E is centrally nilpotent of class at most 2. Our main concern here is with the inner mapping group $\mathfrak{J}$ of E. When H has order 2, E is an abelian group. When H has order 3, complete results on $\mathfrak{J}$ are given in Theorem 1B: *by choice of certain structure constants, $\mathfrak{J}$ may be made isomorphic to any subgroup of G which can be generated by two elements.* As a special consequence we have the existence of a centrally nilpotent loop of order 6, class 2, in contrast with the case for groups. Again, if G and H are isomorphic cyclic groups of any finite odd order n, the structure constants may always be chosen so that $\mathfrak{J}$ is isomorphic to the $(n-1)$th direct power of G, and hence has order n^{n-1} (Theorem 1C). This shows that certain of the results given in §8 of Chapter I are "best possible" in a nontrivial sense.

The culminating result of §2 may be stated as follows (Theorem 2A): *Let $n\geqq 2$ be an arbitrarily assigned integer, and let $G_1, G_2, \cdots, G_n$ be n groups, finite or infinite, each of order at least two, but with G_{n-1} and G_n not both of order two. Then there exists a left-associatrally nilpotent loop E, of class n, with the following properties: If $1=A_0<A_1<\cdots<A_n=E$ is the upper left-associatral series of E, then, for $i=1, 2, \cdots, n$, A_i/A_{i-1} is not only the normal left-associator but also the left-associator of E/A_{i-1}; and A_i/A_{i-1} is isomorphic to G_i.*

Similarly we show in §3 that *if a centrally nilpotent loop E of class n has upper central series $1=Z_i<Z_2<\cdots<Z_n=E$, the only restriction on the abelian groups Z_i/Z_{i-1} $(i=1, 2, \cdots, n)$, aside from the obvious fact that each must contain at least two elements, is that Z_n/Z_{n-1} have order at least three* (Theorem 3A).

In §4 we construct a particularly interesting example of the fact that a characteristic subloop of a loop G need not be normal in G. In the example,

G has order 12, the centrally derived loop G' of G has order 6, and the centrally derived loop G'' of G' has order 2. But G'', though it is a characteristic subloop of G, is not normal in G.

If G is any loop, $\mathfrak{A}$ any group of automorphisms of G, we define the $\mathfrak{A}$-holomorph of G to be the loop consisting of all couples (S, x) with S in $\mathfrak{A}$, x in G under the multiplication $(S, x)(T, y) = (ST, xT \cdot y)$. This definition generalizes the notion of the holomorph of a group. In Theorem 5A the more immediate properties of the $\mathfrak{A}$-holomorph are studied in great detail. It is shown in particular that passage from a loop G to a holomorph preserves the inverse property but not the property of being Moufang. Theorem 5B is concerned with the normal subloops of the $\mathfrak{A}$-holomorph which contain a given $\mathfrak{A}$-admissible normal subloop of G, and Theorem 5C treats of the holomorphs of certain Moufang loops. From the various results we derive examples of associatrally nilpotent and Moufang-nilpotent I.P. loops. Finally, Theorem 5D points out the existence of an I.P. loop whose associator is not a normal subloop, in contrast with the case for Moufang loops.

The general problem discussed in §6 is that of expressing the product operation of one loop in terms of that of another. After some preliminary remarks we consider a Moufang loop G in which $x^{2n+1} = 1$ for every x, where n is a fixed integer. First we prove that the system G_0, consisting of the elements of G under the operation $xoy = (x^2y^{-2})^n x^2$, is a commutative loop (Lemma 6A). A necessary and sufficient condition that G_0 have the inverse property is that $x \cdot y^{-1}xy = y^{-1}xy \cdot x$ for all x, y of G; and in this case we have the simpler expression $xoy = (xy^2x)^{-n}$ (Theorem 6A). Taking G to be a group in which every two conjugate elements commute, we use certain results due to Burnside to prove that G_0 is a commutative Moufang loop, centrally nilpotent of class at most 2 (Theorem 6B). But then, with Theorem 6B at our disposal, we are able to sharpen Burnside's results (Theorem 6C).

§7 is devoted to a study of totally symmetric (or T.S.) quasigroups, namely those in which a valid equation $xy = z$ remains true under all permutations of x, y and z. If (U, V, W) is an autotopism of a T.S. quasigroup G we call the one-to-one transformation U of G upon G an *autotopic* mapping of G. The set of all autotopic mappings forms a group $\mathfrak{H}$, and there exists a uniquely defined endomorphism θ of $\mathfrak{H}$ such that (U, U, U^θ) is an autotopism of G if and only if U is in $\mathfrak{H}$. Those autotopic mappings U which satisfy the equation $xU \cdot y = x \cdot yU$ for all x, y of G form an abelian group $\mathfrak{C}$, a normal subgroup of $\mathfrak{H}$. Every autotopism of G has the form (U, UR, US) where U is in $\mathfrak{H}$, R, S are in $\mathfrak{C}$, and $RS = U^{-1}U^\theta$. The group $\mathfrak{C}$ is of importance in the study of the T.S. isotopes of G. Moreover $\mathfrak{C}$ plays the rôle of a centre for the T.S. quasigroup G, and we may form a "central quotient" quasigroup $G/\mathfrak{C}$. We conclude with an example of a T.S. loop of order 3^n+1 ($n \geqq 2$) with centre of order 1, for which every autotopism is an automorphism; that is, if (U, V, W) is an autotopism, $U = V = W$.

1. **The inner mapping group of a centrally nilpotent loop of class two.** If E is a loop with centre Z and centrally derived loop E', a necessary and sufficient condition that E have class 2 is that $1 < E' \leqq Z < E$ (compare Chapter I, §7). If G is a subloop of E such that $E' \leqq G \leqq Z$ then G, as a subloop of Z, is normal in E (since indeed every element of G is invariant under the inner mapping group of E); moreover E/G is an abelian group since $G \geqq E'$. We shall denote by H an abstract abelian group isomorphic to E/G, written additively, with elements $o, p, q, \cdots$. Further let us suppose that E is written additively, that the elements of G are $o, x, y, \cdots$, and that to each p of H there has been chosen a representative u_p in E, where in particular $u_0 = 0$. Then every element of E will have the form $x + u_p$ for x in G, p in H, where $x + u_p = y + y_q$ if and only if $x = y$, $p = q$. In particular we shall have

$$(1.1) \qquad u_p + u_q = h_{p,q} + u_{p+q},$$

where for each ordered pair p, q of H, $h_{p,q}$ is a uniquely determined element of G. Moreover since G is in Z

$$(1.2) \quad (x + u_p) + (y + u_q) = (x + y) + (u_p + u_q) = (x + y + h_{p,q}) + u_{p+q}$$

for all x, y of G, p, q of G. By setting $p = 0$ in (1.1) we derive $u_q = h_{o,q} + u_q$, or the first of the conditions

$$(1.3) \qquad h_{o,p} = h_{p,o} = 0, \qquad \text{all } p \text{ in } H.$$

The second comes by setting $q = 0$ in (1.1). We have thus proved the concluding statement of the following lemma.

LEMMA 1A. *Let G, H be two abelian groups, written additively, with elements $o, x, y, \cdots$, and $o, p, q, \cdots$, respectively. To every ordered pair of indices p, q of H let there be defined an element $h_{p,q}$ of G, subject to the restriction* (1.3). *Let E be the set of all couples (x, p), x in G, p in H, where $(x, p) = (y, q)$ if and only if $x = y$, $p = q$; and let multiplication be defined in E by*

$$(1.4) \qquad (x, p)(y, q) = (x + y + h_{p,q}, p + q).$$

Then E is a loop; the set (G, o) of all couples (x, o) is a (normal) subloop of E, isomorphic to G and contained in the centre of E; and the corresponding quotient loop $E/(G, o)$ is a loop ısomorphic to H. Conversely if E is a loop with center Z, centrally derived loop E, and if the subloop G of E satisfies $E' \leqq G \leqq Z$, so that E/G is an abelian group H, then E is isomorphic to one of the loops of type (1.4).

Proof. That (1.3), (1.4) define multiplication in a loop follows from the general extension theory (Albert [2], Bruck [2]). That the elements (x, o) form a subloop of the centre may be verified very simply, but it will be convenient for the sequel to proceed as follows. We define A, B, C by

$$(1.5) \qquad A = (x, p), \qquad B = (y, q), \qquad C = (z, r).$$

With the usual meanings for the permutations R_A, L_A, and so on, we see from (1.4) that

$$(1.6)\quad AR_B = (x + y + h_{p,q},\ p + q),\quad AL_B = (x + y + h_{q,p},\ p + q).$$

Hence

$$(1.7)\quad AR_B^{-1} = (x - y - h_{p-q,q},\ p - q),\quad AL_B^{-1} = (x - y - h_{q,p-q},\ p - q),$$

as we may verify, for example, by computing $AR_B^{-1}R_B$. A perfectly straightforward calculation shows that if $R_{B,C} = R_B R_C R_{BC}^{-1}$, $L_{B,C} = L_B L_C L_{BC}^{-1}$, $T_B = R_B L_B^{-1}$ then

$$(1.8)\quad AR_{B,C} = (x + a_{p,q,r},\ p),\quad AL_{B,C} = (x + b_{p,q,r},\ p),\quad AT_B = (x + c_{p,q},\ p)$$

where

$$(1.9)\quad \begin{aligned} a_{p,q,r} &= h_{p,q} + h_{p+q,r} - h_{q,r} - h_{p,q+r}; \qquad c_{p,q} = h_{p,q} - h_{q,p};\\ b_{p,q,r} &= h_{q,p} + h_{r,p+q} - h_{r,q} - h_{q+r,p} = - a_{r,q,p}. \end{aligned}$$

We note that (1.3) and (1.9) imply

$$(1.10)\qquad a_{o,q,r} = a_{p,o,q} = a_{p,q,o} = b_{o,q,r} = c_{o,q} = 0,$$

for all p, q, r. Now $R_{B,C}$, $L_{B,C}$, T_B and their inverses generate the inner mapping group $\mathfrak{J}$ of E, and an element $A = (x, p)$ is in the centre of E if and only if $AU = A$ for every U of $\mathfrak{J}$. Hence, by (1.8), (1.10), (x, o) is in the centre for every x of G. That the elements (x, o) form a loop (G, o) isomorphic to G, and that the quotient loop $E/(G, o)$ is isomorphic to H, are also consequences of the general extension theory for loops. This completes the proof of Lemma 1A.

Now $AB \cdot C = A \cdot BC$ for all A, B, C of the loop E if and only if $AR_{B,C} = A$ for all A, B, C, or, by (1.8), if and only if $a_{p,q,r} = 0$ for all p, q, r of H. Hence we may state a well known lemma.

LEMMA 1B. *A necessary and sufficient condition that the loop E, defined by* (1.4), *should be a group is that*

$$(1.11)\qquad h_{p,q} + h_{p+q,r} = h_{q,r} + h_{p,q+r}$$

for all p, q, r of H.

Similarly, E is commutative if and only if $AB = BA$ or $AT_B = A$ for all A, B of E. Hence:

LEMMA 1C. *A necessary and sufficient condition that the loop E defined by* (1.4) *should be commutative is that $h_{p,q} = h_{q,p}$ for all p, q of H.*

Consider the mapping M of E upon E, defined by

$$(1.12)\qquad (x, p)M = (x + t_p,\ p)$$

where the t_p are elements of G, arbitrary except for the restriction $t_0=0$. With A, B as in (1.5) we have $(AB)M=(x+y+h_{p,q}+t_{p+q}, p+q)$, $(AM)(BM)=(x+y+h_{p,q}+t_p+t_q, p+q)$. Now the mapping M is clearly one-to-one, for every choice of the t_p. From (1.13) we therefore derive the following:

Lemma 1D. *A necessary and sufficient condition that the mapping M, defined by* (1.12), *should be an automorphism of the loop E, defined by* (1.4), *is that*

$$(1.13) \qquad t_{p+q} = t_p + t_q$$

for all p, q of H.

From (1.12) and (1.7) we obtain

$$(1.14) \qquad AML_A^{-1} = (t_p, o).$$

But the set of elements (1.14), obtained by letting M range over the set of all permutations $R_{B,C}$, L_B,C and T_B, generate the centrally derived loop E' of E (Chapter I, §3 and Lemma 7C). Moreover the mapping $M\rightarrow(t_p, o)$ induces a homomorphism of the inner mapping group $\mathfrak{J}$ of E upon a subgroup G_p of G. We may go further:

Theorem 1A. *Let $E=(G, H)$ be the centrally nilpotent loop, of class at most two, defined by* (1.3) *and* (1.4). *Let E', $\mathfrak{J}$ be respectively the centrally derived loop and the inner mapping group of E. In addition let G_p, for each fixed p of H, be the subgroup of G generated by the elements $a_{p,q,r}$, $b_{p,q,r}$, and $c_{p,q}$, where q, r range over H. Then E' and $\mathfrak{J}$ are respectively isomorphic to the union and to a subgroup of the direct product of the set of all groups G_p for p in H.*

Corollary. *If G is a cyclic group, and if E has class* 2, *E' is isomorphic to G and $\mathfrak{J}$ to a direct power of G.*

Proof. That E' is isomorphic to the union of the G_p is obvious. The fact about $\mathfrak{J}$ represents only a slight sharpening (the proof being unchanged) of Lemma 8B of Chapter I. The corollary follows immediately.

Lemma 1E. *There exists no centrally nilpotent loop with central quotient group of order* 2.

Proof. Let H have order two, elements 0, 1. Then clearly $c_{p,q}=0$ and $a_{p,q,r}=0$ for all p, q, r, since $a_{1,q,1}=0$. Thus $E=(G, H)$ is an abelian group.

Theorem 1B. *In the notation of Theorem* 1A, *let H be the additive cyclic group of order three* (*elements* 0, 1, 2), *and let F be the subgroup of G generated by the elements $h_{1,1}+h_{2,2}-h_{1,2}$, $h_{1,2}-h_{2,1}$. Then E' and $\mathfrak{J}$ are respectively isomorphic to F and $F\times F$. Moreover the subgroup of $\mathfrak{J}$ consisting of the "inner" automorphisms of E is isomorphic to the subgroup of F consisting of all elements of F of order* 3.

Corollary 1. *If the abelian group G can be generated by two elements, the*

$h_{p,q}$ can be chosen so that E' and $\mathfrak{J}$ are respectively isomorphic to G and $G\times G$.

COROLLARY 2. *There exists a centrally nilpotent loop of class 2, order 6 (the smallest possible order).*

COROLLARY 3. *Not every finite centrally nilpotent loop is a direct product of p-loops.*

Proof. If M is defined by (1.12) with $t_0=0$, the mapping $M\rightarrow(t_1, t_2)$ induces an isomorphism of $\mathfrak{J}$ into the group $G\times G$, the elements of the latter being written as couples. At this stage it will be convenient to write $R_{q,r}$ instead of $R_{B,C}$, for example, since the latter mapping depends only on q, r when $B=(y, q)$, $C=(z, r)$. With a similar notation for the other generators of $\mathfrak{J}$ we may verify that, in the above-mentioned isomorphism of $\mathfrak{J}$ into $G\times G$,

$$\overset{-1}{T_1} \rightarrow (0,\ h_{12} - h_{21}), \qquad T_2 \rightarrow (h_{12} - h_{21},\ 0).$$

$$R_{21} = \overset{-1}{R_{11}} \rightarrow (h_{12} - h_{21},\ h_{11} + h_{22} - h_{21}),$$

$$R_{12} = \overset{-1}{R_{22}} \rightarrow (h_{11} + h_{22} - h_{21},\ h_{21} - h_{12}),$$

$$L_{21} = \overset{-1}{L_{11}} \rightarrow (h_{21} - h_{12},\ h_{11} + h_{22} - h_{12}),$$

$$L_{12} = \overset{-1}{L_{22}} \rightarrow (h_{11} + h_{22} - h_{21},\ h_{12} - h_{21}).$$

As a consequence, the image of $\mathfrak{J}$ in $G\times G$ has as its generators the couples $(h_{12}-h_{21},\ 0)$, $(h_{11}+h_{22},\ 0)$, $(0,\ h_{12}-h_{21})$ and $(0,\ h_{11}+h_{22}-h_{12})$. Thus $\mathfrak{J}$ is isomorphic to $F\times F$, where F is defined as in the theorem. Moreover $G_0=0$, $G_1=G_2=F$, in the notation of Theorem 1A, and hence E' is isomorphic to F.

As to the last statement of Theorem 1B, if the mapping M, defined by (1.12), is an automorphism of E, then, by Lemma 1D, $t_{p+q}=t_p+t_q$, from which we find $t_1+t_2=0$ and $3t_1=0$. Thus $U\in\mathfrak{J}$ is an inner automorphism of E if and only if its image, in the isomorphism of the previous paragraph, is of form $(t, -t)$ with t in F and $3t=0$.

The corollaries seem to be immediate. Perhaps we should remark, in connection with Corollary 3, that a loop of order 6, for example, can be a direct product of finite p-loops if and only if it is an abelian group.

THEOREM 1C. *In the notation of Theorem 1A, let G and H be (isomorphic) cyclic groups, each of finite odd order n. Then the $h_{p,q}$ may be chosen so that $\mathfrak{J}$ has (maximum possible) order n^{n-1} and is in fact isomorphic to the $(n-1)$th direct power of G.*

Proof. Without loss of generality we may assume that G and H are identical with the additive group consisting of the integers $0, 1, 2, \cdots, n-1$, taken modulo n. Then let us set

$$(1.15) \qquad h_{0,q} \equiv 0, \qquad h_{p,q} \equiv q \qquad \text{for } p \not\equiv 0 \pmod{n}.$$

Under the present circumstances the mapping $M\rightarrow(t_1, t_2, \cdots, t_{n-1})$ induces an isomorphism of $\mathfrak{J}$ into the $(n-1)$th direct power of G. (Compare the proof of the previous theorem.) It may be verified from (1.9) and (1.15) that, if p, r, and $r-1$ are incongruent to zero modulo n, $a_{p,-1,-r}-a_{p,-r,-r}\equiv 2r$, $-2r$, or 0 (mod n) according as $p\equiv 1$, $p\equiv r$, or $p\not\equiv 1$, r. Thus in the isomorphism induced by $M\rightarrow(t_1, t_2, \cdots, t_{n-1})$, $R_{-1,-r}R_{-r,-r}^{-1}$ is mapped into such a symbol with $t_1\equiv 2r$, $t_r\equiv -2r$, $t_p\equiv 0$ otherwise. Since G is cyclic it follows that the isomorphic image of $\mathfrak{J}$ contains the symbols $(1, -1, 0, \cdots)$, $(1, 0, -1, 0, \cdots)$, $\cdots$, $(1, 0, 0, \cdots, -1)$. Thus if $t_2, t_3, \cdots, t_{n-1}$ are any integers, the image of $\mathfrak{J}$ also contains $(t_2+\cdots+t_{n-1}, -t_2, -t_3, \cdots, -t_{n-1})$ and in particular—the case $t_p\equiv 2-p$, $p=2, \cdots, n-1$—the symbol $(3, 0, 1, 2, \cdots, n-3)$. But, for $p\neq 0$, $c_{p,2}=2-p$ and so $T_2^{-1}\rightarrow(-1, 0, 1, 2, \cdots, n-3)$. By subtraction we see that the image of $\mathfrak{J}$ contains $(4, 0, 0, \cdots, 0)$ and hence $(1, 0, 0, 0, \cdots)$, $(0, 1, 0, 0, \cdots)$, $\cdots$. Thus $\mathfrak{J}$ is isomorphic to the $(n-1)$th direct power of G, and has order n^{n-1}.

Corollary 1. *If, under the hypotheses of Theorem* 1C, *the $h_{p,q}$ are chosen in any manner so that $\mathfrak{J}$ has order n^{n-1}, the group of "inner" automorphisms of the loop $E=(G, H)$ has order n.*

Proof. Since G is cyclic, it follows by Lemma 1D that a mapping M of type (1.12) is an automorphism of E if and only if $t_p=pt$, $p=2, 3, \cdots, n-1$. The group of all automorphisms of this type is thus isomorphic with G. But these automorphisms M will certainly all be "inner" (that is, contained in $\mathfrak{J}$) when $\mathfrak{J}$ has order n^{n-1}.

Corollary 2. *There exist centrally nilpotent p-loops of class* 2, *order p^{2m}, for every odd prime p and for every positive integer m; and at least one of those of order p^{2m} has an inner mapping group of order p^q where $q=m(p^m-1)$.*

Proof. This corollary follows from Theorem 1C with $n=p^m$. The case of special interest is $m=1$, since every *group* of order p^2 is an abelian group (and hence has class 1). Note that this case $(m=1)$ also illustrates the fact that the centrally derived loop of a finite centrally nilpotent p-loop may have index as small as p, in contrast with the case for groups. Since every loop of order $2^2=4$ is known to be an abelian group, the restriction to odd primes is essential.

2. **Construction of left-associatrally nilpotent loops of arbitrary class.** Let E be a loop, written multiplicatively, with a normal subloop G contained in the left associator. Let the loop E/G be isomorphic to a loop H, written multiplicatively, with elements $1, p, q, \cdots$, and suppose that to each element p of H there has been chosen a representative u_p in E such that $u_1=1$. Finally let the elements of G be $1, x, y, \cdots$. Since G is in the left associator, $xu_p\cdot yu_q=x\cdot(u_p\cdot yu_q)$. Again, since G is normal in E, $u_p\cdot yu_q=(yS_{p,q})\cdot(u_pu_q)$, where $S_{p,q}$ is in the inner mapping group of E, and where in particular $S_{1,q}=I$, the identity mapping, for all q of H. Of course

$yS_{p,q}$ is in G, and also $1S_{p,q}=1$, for all p, q of H. Thus $xu_p \cdot yu_q = x\cdot(yS_{p,q}\cdot u_pu_q) = (x\cdot yS_{p,q})\cdot u_pu_q$. Finally, there must exist an element $h_{p,q}$ of G, corresponding to every ordered pair of elements p, q of H, such that $u_pu_q = h_{p,q}\cdot u_{pq}$ and also $h_{1,p}=h_{p,1}=1$ for all p of H. Since G, as a subloop of the left associator, is a group, we have proved the concluding statement of the following lemma.

LEMMA 2A. *Let G be a group with elements $1, x, y, \cdots$, H a loop with elements $1, p, q, \cdots$, each written multiplicatively. Corresponding to every ordered pair p, q of elements of H let there be chosen a one-to-one mapping $S_{p,q}$ of G upon G, and an element $h_{p,q}$ of G, subject to the following restrictions:*

$$(2.1) \qquad 1S_{p,q} = h_{p,1} = h_{1,q} = 1 \qquad \textit{for all } p, q \textit{ of } H;$$

$$(2.2) \qquad S_{1,q} = I, \textit{ the identity mapping}, \qquad \textit{for all } q \textit{ of } H.$$

Further let $E=(G, H; S_{p,q}, h_{p,q})$ be the set of all couples (x, p) with x in G, p in H, where $(x, p)=(y, q)$ if and only if $x=y$, $p=q$; and let multiplication be defined in E by

$$(2.3) \qquad (x, p)(y, q) = (x\cdot yS_{p,q}\cdot h_{p,q}, pq).$$

Then E is a loop with unit $(1, 1)$; the set $(G, 1)$ of all elements $(x, 1)$ is a normal subloop of E, isomorphic to G and contained in the left associator of E; and the quotient loop $E/(G, 1)$ is isomorphic to H. Furthermore every loop E with a normal subloop G contained in the left associator and with quotient loop E/G isomorphic to H is isomorphic to such a loop $(G, H; S_{p,q}, h_{p,q})$.

Proof. We leave it to the reader to verify that

$$(2.4) \qquad [(x, 1)(y, q)](z, r) = (xy\cdot zS_{q,r}\cdot h_{q,r}, qr) = (x, 1)[(y, q)(z, r)]$$

for all x, y, z of G and q, r of H. The rest of the proof follows easily.

LEMMA 2B. *Let $E=(G, H; S_{p,q}, h_{p,q})$ be a loop constructed as in Lemma 2A, where G and H have orders at least two. If G, H both have order two, E is an abelian group; but otherwise the $S_{p,q}$ and $h_{p,q}$ can always be chosen so that the left associator of E is precisely $(G, 1)$.*

Proof. If both G and H have at least three elements we may set $h_{p,q}=1$ for all p, q of H and define the $S_{p,q}$ as follows:

$$(2.5) \qquad S_{1,q} = I; \qquad S_{p,q} = S_q \text{ for } p \rightarrow 1; \qquad S_1 = I,$$

where we choose the S_q so that, for each $q\neq 1$ of H, S_q is a nontrivial automorphism of G. (This is always possible[18] when the order of G is greater than 2.) With this choice we have

[18] A little thought will convince the reader that the only troublesome case is when G is a non-denumerable abelian group in which every element save the identity has order 2. This case may be handled with the help of the axiom of choice.

$$(2.6) \qquad (x, p)(y, q) = (x \cdot yS_q, pq) \qquad \text{for } p \neq 1.$$

Now we shall show that (x, p) is in the left associator of E if and only if $p=1$. Assume in fact $p\neq 1$, and choose q so that $q\neq 1$, $pq\neq 1$. (This is always possible since H has order greater than 2.) Then, since $pq\neq 1$, we have from (2.5), (2.6) that $[(x, p)(y, q)](z, 1) = (x\cdot yS_q\cdot z, pq)$. But $(y, q)(z, 1) = (yz, q)$ and so $(x, p)[(y, q)(z, 1)] = (x\cdot (yz)S_q, pq) = (x\cdot yS_q\cdot zS_q, pq)$. Since S_q is a nontrivial automorphism we may choose z so that $z\neq zS_q$. Thus (x, p) is not in the left associator of E for $p\neq 1$. But every $(G, 1)$ is in the left associator, by Lemma 2A. This proves the point at issue.

Again, if G has at least three elements but H has order two, elements 1, e, we set $h_{p,q}=1$ for all p, q of H and let $S_{e,e}=S$ be a nontrivial automorphism of G. We wish to show that (x, e) is not in the left associator of E. In this case $[(x, e)(y, e)](z, 1) = (x\cdot yS\cdot z, 1)$, but $(x, e)[(y, e)(z, 1)] = (x\cdot (yz)S, 1) = (x\cdot yS\cdot zS, 1)$; and we can always choose z so that z and zS are distinct.

Note that we have shown incidentally that if G has order at least three and H order at least two, not only is Lemma 2B correct but there exist, moreover, three elements (x, p), (y, q), and $(z, 1)$ of E such that $[(x, p)(y, q)](z, 1) \neq (x, p)[(y, q)(z, 1)]$. This leads to the following corollary.

COROLLARY TO LEMMA 2B. *If G and H have orders not less than three and two respectively, the $S_{p,q}$ and $h_{p,q}$ may be so chosen that $(G, 1)$ is precisely the left associator of E and is, moreover, not wholly contained in the right associator of E.*

If the group G has order 2 we must proceed a little differently. For if G has elements 1, e (with $e^2=1$) and if S is a one-to-one mapping of G upon G, $1S=1$ implies $eS=e$. Thus (2.3) becomes

$$(2.7) \qquad (x, p)(y, q) = (x\dot{y}h_{p,q}, pq),$$

so that $(G, 1)$ is, in fact, contained in the centre of E. In this case suppose H has order at least three and set $h_{p,q}=e$ for p, $q\neq 1$, $h_{p,q}=1$ otherwise. If $p\neq 1$ is given, choose q so that $pq=1$ (and hence $q\neq 1$), and choose r (as is possible) so that $r\neq 1$, $qr\neq 1$. Then $(x, p)(y, q) = (xye, 1)$ and $[(x, p)(y, q)](z, r) = (xyze, r)$; but $(y, q)(z, r) = (yze, qr)$ and $(x, p)[(y, q)(z, r)] = (xyz, p\cdot qr)$. Hence comparison of the left-hand components, $xyze$ and xyz, shows that (x, p) is not in the left associator.

Finally, it is well known that every loop of order four is an abelian group. This completes the proof of Lemma 2B.

Now let $n\geqq 2$ be an arbitrarily assigned integer, and let $G_1, G_2, \cdots, G_n$ be n groups, finite or infinite, but each of order at least two. Assume moreover that G_{n-1} and G_n are not both of order two. Define a sequence of loops E_i as follows: $E_0=1$; $E_1=(G_n, E_0)=G_n$; $E_i=(G_{n+1-i}, E_{i-1})$ for $2\leqq i\leqq n$, such that the left associator F_i of E_i is a normal subloop isomorphic to G_{n+1-i}, and E_i/F_i is isomorphic to E_{i-1}. (This is possible, in view of Lemmas 2A, 2B.) Now let $E=E_n$. It follows that there exists a strictly increasing series

$1=A_0<A_1< \cdots <A_n=E$ of normal subloops of E such that A_i/A_{i-1} is the left associator of E/A_{i-1} and A_i/A_{i-1} is isomorphic to G_i, for $i=1, 2, \cdots, n$. In fact if A_1 is the associator of E, $A_1/A_0=A$ is normal in $E=(G_1, E_{n-1})$ and isomorphic to G_1, and E/A_1 is isomorphic to $E_{n-1}=(G_2, E_{n-2})$. The rest of the proof follows by induction. Thus we have obtained the following theorem.

THEOREM 2A. *Let $n\geqq 2$ be an arbitrarily assigned integer, and let $G_1, G_2, \cdots, G_n$ be n groups, finite or infinite, each of order at least two, but with G_{n-1} and G_n not both of order two. Then there exists a left-associatrally nilpotent loop E, of class n, with the following properties: If $1=A_0<A_1< \cdots <A_n=E$ is the upper left-associatral series of E, then for $i=1, 2, \cdots, n$, A_i/A_{i-1} is not only the normal left associator but also the left associator of E/A_{i-1}; and A_i/A_{i-1} is isomorphic to G_i.*

It should be remembered that the restriction of G_{n-1}, G_n to groups not both of order two is essential. (Compare Lemma 2B.)

Wholly analogous results may of course be given for right-associatral series, but new problems arise in the cases of middle-associatral and associatral series. The theory of the latter is in fact roughly of the same order of difficulty as the extension theory of non-commutative groups.

3. **Centrally nilpotent loops of arbitrary class.** With the detailed work of the two preceding sections as background, we may now proceed more informally. If G is a (multiplicative) abelian group of order at least two, with elements $1, x, y, \cdots$, every loop F which contains G as a normal subloop of its centre is isomorphic to a loop E consisting of couples (x, p), where p is an element of the (multiplicative) loop $G/E=H$, and where

$$(x, p)(y, q) = (xyh_{p,q}, pq). \tag{3.1}$$

Here the $h_{p,q}$ are arbitrary elements of G, subject only to the restrictive

$$h_{1,p} = h_{p,1} = 1. \tag{3.2}$$

Now if H has order two, E is an abelian group, by Lemma 1E; hence we shall assume that H has at least three elements.

We now wish to prove that the $h_{p,q}$ may be chosen so that $(G, 1)$ is precisely the centre of $E=(G, H)$. It is convenient to distingush two cases. If G has an element $e\neq 1$ of order two, set $h_{p,q}=e$ for $p\neq 1$, $q\neq 1$, $h_{p,q}=1$ otherwise, and proceed as in the latter part of the proof of Lemma 2B: Given $p\neq 1$, pick $q\neq 1$ so that $pq=1$, and pick $r\neq 1$ so that $qr\neq 1$. Then $[(x, p)(y, q)](z, r)=(xyze, r)$ but $(x, p)[(y, q)(z, r)]=(xyz, r)$, so that (x, p) is not in the centre of E.

On the other hand, if G has an element $e\neq 1$, not of order two, we may instead set $h_{p,q}=e$ provided $p\neq 1$, $q\neq 1$, $pq\neq 1$, and $h_{p,q}=1$ otherwise. In this case, given $p\neq 1$, choose q and r exactly as above. This time we find $[(x, p)(y, q)](z, r)=(xyz, r)$ and $(x, p)[(y, q)(z, r)]=(xyze^2, p\cdot qr)$, so the conclusion still holds. We now may state a theorem.

THEOREM 3A. *Let $n \geqq 2$ be an arbitrarily assigned integer, and let $G_1, G_2, \cdots, G_n$ be n abelian groups, finite or infinite, each of order at least two, but with G_n of order at least three. Then there exists a centrally nilpotent loop E, of class n, with the following property: If $1 = Z_0 < Z_1 < \cdots < Z_n = E$ is the upper central series of E, then Z_i/Z_{i-1} is isomorphic to G_i for $i = 1, 2, \cdots, n$.*

The proof of Theorem 3A is wholly analogous to that of Theorem 2A. As previously remarked, the restriction on G_n follows from Lemma 1E: the centre Z_{n-1}/Z_{n-2} cannot have index two in the centrally nilpotent loop Z_n/Z_{n-2} of class 2.

4. **Characteristic subloops need not be normal.** It is known that characteristic subloops of a loop need not be normal, and an example has already been given in this paper (Chapter II, §3) of a loop with a non-normal left associator. In view of the great importance of the point at issue it seems worthwhile to present here an example of a different type.

Let G be a centrally solvable loop with centrally derived loop G', and let G'' be the centrally derived loop of G'. Now G' is a characteristic subloop of G, in view of its definition, and G'', as a characteristic subloop of G', is also characteristic in G. Thus G' is normal in G, and G'' normal in G'; but we shall construct G so that G' is not normal in G.

Since G' has composite order, and is not an abelian group, G' must have order at least 6, and hence G must have order at least 12. Therefore let the elements of the proposed loop G be $1, 2, \cdots, 12$, where 1 is the unit element, and let the multiplication table of G be written in the form

$$\begin{array}{|cc} \hline A & B \\ B & C \end{array}$$

where the elements $1, \cdots, 12$ are to be written in order in the sideline and headline, and where A, B, C are 6×6 latin squares whose construction will be explained. In particular we let A, including the corresponding part of the sideline and headline, be given by

(4.1)

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	3	6	5
3	3	4	6	5	2	1
4	4	3	5	6	1	2
5	5	6	2	1	4	3
6	6	5	1	2	3	4

To form B we write the elements $7, 8, \cdots, 12$ in natural order in the first row, and permute them cyclically in subsequent rows. Finally, for C we take any latin square on the elements $1, 2, \cdots, 6$.

Clearly G is a loop with unit 1. The set H, consisting of the elements $1, 2, \cdots, 6$, is a subloop of G, as is clear from (4.1). But H has index 2 in G, and hence is normal (Albert [2]); and of course G/H is the 2-group, so $H \geqq G'$. It is readily verified from (1.2) that the only nontrivial subloop of H is $K=(1, 2)$; moreover K is a normal subloop of H, since the cosets $K=(1, 2)$, $3K=(3, 4)$ and $5K=(5, 6)$ form the cyclic group of order 3. However, K is not normal in G, since for example $7K=(7, 8)$ but $8K=(8, 9)$. Thus H is the only proper normal subloop of G which contains G', so $H=G'$, and K is the only proper normal subloop of H, so $K=H'=G''$. Hence G'' is not normal in G.

5. **The holomorphs of a loop.** Let G be any loop, $\mathfrak{A}$ any group of automorphisms of G, and denote by $(\mathfrak{A}, G)$ the set of all couples (S, x) with S in $\mathfrak{A}$, x in G, under the multiplication

$$(5.1) \qquad (S, x)(T, y) = (ST, xT \cdot y).$$

Then $(\mathfrak{A}, G)$ is a loop, which we shall call the $\mathfrak{A}$-*holomorph* of G.

When G is a group and $\mathfrak{A}$ is the group of all automorphisms of G, $(\mathfrak{A}, G)$ is isomorphic to the holomorph of G—used extensively by many early writers on group theory—as will be seen from parts (i), (ii), and (iii) of the following theorem. We designate by 1 both the unit of $\mathfrak{A}$ and the unit of G. Moreover, if $\mathfrak{B}$, K are any subsets of $\mathfrak{A}$, G respectively, we denote by $(\mathfrak{B}, K)$ the set of all elements (S, x) with S in $\mathfrak{B}$, x in K. Clearly $(1, G)$ is isomorphic to G, and $(\mathfrak{A}, 1)$ to $\mathfrak{A}$.

THEOREM 5A. *If $E=(\mathfrak{A}, G)$ is the $\mathfrak{A}$-holomorph of the loop G, then:*

(i) *$(1, G)$ is a normal subloop of E, and $E/(1, G)$ is isomorphic to $\mathfrak{A}$;*

(ii) *if K is the associator of G, $(\mathfrak{A}, K)$ is the associator of $(\mathfrak{A}, G)$; thus E is a group if and only if G is a group;*

(iii) *every $\mathfrak{A}$-automorphism of $(1, G)$ is induced by an inner automorphism of E; specifically, $(S, 1)^{-1}(1, x)(S, 1)=(1, xS)$;*

(iv) *E is an I.P. loop if and only if G is an I.P. loop;*

(v) *if G is an I.P. loop with Moufang nucleus M, and if N is the set of all x of M such that xSL_x^{-1} is in the associator of G for every S of $\mathfrak{A}$, then $(\mathfrak{A}, N)$ is the Moufang nucleus of the I.P. loop E;*

(vi) *if G is an I.P. loop with Moufang nucleus M, the Moufang centre of the I.P. loop E consists of all elements of form (U, u) where $u \in M$ satisfies $uS=u$ for all S of $\mathfrak{A}$ and where $U \in \mathfrak{A}$ satisfies $xU=uxu^{-1}$ for all x of G. Incidentally U is unique when it exists, and lies in the centre of $\mathfrak{A}$.*

Remarks. Part (ii) of Theorem 5A shows how to construct loops with nontrivial associators. Moreover (v) demonstrates the existence of an I.P. loop with a nontrivial Moufang nucleus; we can for example take G to be a commutative Moufang loop, centrally nilpotent of class 3, and let $\mathfrak{A}$ be the inner mapping group of G.

Proof. (i) This follows from the general extension theory.

(ii) By use of (5.1) we find that $[(S, x)(T, y)](U, z)=(S, x)[(T, y)(U, z)]$ if and only if $(xTU\cdot yU)z=xTU\cdot(yU\cdot z)$. Since the various associators of G are characteristic subloops of G it follows that (S, x) is in the left associator of E if and only if x is in the left associator of E; that (T, y) is in the middle associator of E if and only if y is in the middle associator of G; and that (U, z) is in the right associator of E if and only if z is in the right associator of G. But (ii) is an immediate consequence of these facts and of the definition of the associator.

(iii) By (ii), $(S, 1)$ is in the associator of E for every S. It follows that the mapping $(T, x)\rightarrow(S, 1)^{-1}(T, x)(S, 1)=(S^{-1}TS, xS)$ is an inner automorphism of E. Taking $T=1$, we get the result stated.

(iv) If E is an I.P. loop, $(1, G)$ and hence G are I.P. loops. If G is an I.P. loop, we note from (5.1) that we should define

$$(5.2)\qquad (S, x)^{-1} = (S^{-1}; (x^{-1})S^{-1}).$$

But then $(S, x)^{-1}[(S, x)(T, y)]=(T, y)=[(T, y)(S, x)](S, x)^{-1}$, and so E has the inverse property.

(v) (S, x) is in the Moufang nucleus of the I.P. loop E if and only if $\{(S, x)[(T, y)(U, z)]\}(S, x)=[(S, x)(T, y)][(U, z)(S, x)]$ for all T, U, y, z; or, equivalently, if and only if $(xV\cdot yz)x=(xV\cdot y)(zx)$ for all V of A. In other words, $(L_{xV}, R_x, L_{xV}R_x)$ must be an autotopism of G for all V. The case $V=1$ says (L_x, R_x, L_xR_x) is an autotopism; and hence $(L_{xV}L_x^{-1}, I, L_{xV}L_x^{-1})$ must be an autotopism; that is, $1L_{xV}L_x^{-1}=xVL_x^{-1}$ must lie in the associator of the I.P. loop G. The converse gives no trouble. From these facts (v) follows immediately.

(vi) We remind the reader that the Moufang centre of an I.P. loop E consists of those elements of the Moufang nucleus which commute with every element of E. Thus if (U, u) is in the Moufang center of E, u must be in N (in the notation of (v)) and hence in M. Further, we must have $(U, u)(S, x)=(S, x)(U, u)$ for all S, x, from which we derive the two conditions

$$(5.3)\qquad US = SU,\qquad uS\cdot x = xU\cdot u.$$

We ignore the first condition for the moment. From the second, with $S=1$, we derive $ux=xU\cdot u$, or, since the product uxu^{-1} is unambiguous when u is in M,

$$(5.4)\qquad xU = uxu^{-1}$$

for all x. From (5.3), (5.4) we derive $uS\cdot x=ux$ or $uS=u$ for all S.

Conversely, if u is in M, and if $uS=u$ for all S, then $uSL_u^{-1}=1$ for all S, whence, by (v), u is in N. If, further, there exists a U of $\mathfrak{A}$ which satisfies

(5.4), U is clearly unique. But, moreover, $x(S^{-1}US)=(u\cdot xS^{-1}\cdot u^{-1})S=uxu^{-1}=xU$, and hence $S^{-1}US=U$, $US=SU$ for all S. Thus both conditions (5.3) are satisfied for all S, x; and, since u is in N, (U, u) is in the Moufang centre of E.

DEFINITION. If $\mathfrak{A}$ is a group of automorphisms of a loop G, we shall say that a subset H of G is $\mathfrak{A}$-admissible if and only if xS is in H for every x of H and S of $\mathfrak{A}$.

THEOREM 5B. *Let $(\mathfrak{A}, G)$ be the $\mathfrak{A}$-holomorph of the loop G, and let H be an $\mathfrak{A}$-admissible normal subloop of G. Then:*

(i) *if $\mathfrak{B}$ is a subset of $\mathfrak{A}$, $(\mathfrak{B}, H)$ is a normal subloop of $(\mathfrak{A}, G)$ if and only if $\mathfrak{B}$ is a normal subgroup of $\mathfrak{A}$ with the property that xUL_x^{-1} is in H for every x of G and U of $\mathfrak{B}$;*

(ii) *the subset $\mathfrak{B}$ of $\mathfrak{A}$, consisting of all U of $\mathfrak{A}$ such that xUL_x^{-1} is in H for every x of G, is a normal subgroup of $\mathfrak{A}$.*

(iii) *if $\mathfrak{B}$ is the normal subgroup of $\mathfrak{A}$ defined in* (ii), *the quotient group $\mathfrak{A}/\mathfrak{B}$ is isomorphic to a group of automorphisms $\mathfrak{C}$ of the quotient loop G/H, and $(\mathfrak{A}, G)/(\mathfrak{B}, H)$ is isomorphic to the $\mathfrak{C}$-holomorph $(\mathfrak{C}, G/H)$ of G/H.*

Proof. (i) By Lemma 3A of Chapter I, $(\mathfrak{B}, H)$ is a normal subloop of $(\mathfrak{A}, G)$ if and only if, for every assigned pair of elements (S, x), (T, y) of $(\mathfrak{A}, G)$, the equation

$$[(U, a)(S, x)][(V, b)(T, y)] = (W, c)[(S, x)(T, y)]$$

ensures that all three of (U, a), (V, b), (W, c) are in $(\mathfrak{B}, H)$ whenever two are. But this equation is equivalent to the two equations

$$USVT = WST; \tag{5.5}$$

$$(aSVT\cdot xVT)(bT\cdot y) = cST\cdot(sT\cdot y). \tag{5.6}$$

It follows from (5.5), with $S=T=1$, that $\mathfrak{B}$ must be a subgroup of $\mathfrak{A}$. Again, (5.5) may be written as $SVS^{-1}=U^{-1}W$, whence we see that $\mathfrak{B}$ must be normal in $\mathfrak{A}$. Since $H=H\mathfrak{A}$ is normal in G, (5.6) implies $(H\cdot xVT)(Hy)=H(xT\cdot y)=(H\cdot xT)(Hy)$. Thus $(H\cdot xVT)=H\cdot xT$, or $H\cdot xV=Hx$. This is equivalent to stating that xV is in $Hx=xH$, or that xVL_x^{-1} is in H, for every V of $\mathfrak{B}$ and x of G.

Conversely, if $\mathfrak{B}$ is a normal subloop of $\mathfrak{A}$, the conditions in connection with (5.5) are satisfied. And if, further, xUL_x^{-1} is in H for every x of G, U of $\mathfrak{B}$, then a is in H if and only if $aSVT\cdot xVT$ is in $H\cdot xVT=(H\cdot xV)T=H\cdot xT$; b is in H if and only if $bT\cdot y$ is in Hy; c is in H if and only if $cST\cdot(xT\cdot y)$ is in $H(xT\cdot y)=(H\cdot xT)(Hy)$. Thus, in this case, the conditions in connection with (5.6) are also verified. This completes the proof of (i).

(ii) We note that xUL_x^{-1} is in H for all x if and only if $H\cdot xU=H\cdot x$ for all x. If U has this property so does U^{-1}, since $H\cdot xU^{-1}=(Hx)U^{-1}=(H\cdot xU)U^{-1}=H\cdot x$; and if U, V have this property, so does UV, since

$H\cdot xUV=(H\cdot xU)V=(Hx)V=H\cdot xV=Hx$. Finally, if $H\cdot xU=Hx$ for all x, $H\cdot x(S^{-1}US)=[H\cdot(xS^{-1})U]S=(H\cdot xS^{-1})S=Hx$. Thus the set $\mathfrak{B}$ consisting of all U of $\mathfrak{A}$ such that $H\cdot xU=Hx$ for all x is a normal subgroup of $\mathfrak{A}$.

(iii) If $\mathfrak{B}$ is defined as in (ii), and if we define a group $\mathfrak{C}$ of automorphisms S' of G/H by setting $(Hx)S'=H\cdot xS$, it is clear at once that the homomorphism $S\rightarrow S'$ of $\mathfrak{A}$ upon $\mathfrak{C}$ has kernel $\mathfrak{B}$. If, as is convenient, we write the cosets of $(\mathfrak{A}, G)/(\mathfrak{B}, H)$ in the form $(S, x)(\mathfrak{B}, H)=(S\mathfrak{B}, xH)=(S', xH)$, it follows that $(S', xH)(T', yH)=(S'T', [xH]T'\cdot yH)$. This completes the proof.

Theorem 5C. *Let G be a Moufang loop whose inner mapping group $\mathfrak{I}$ is a group of automorphisms; and let $E=(\mathfrak{I}, G)$ be the $\mathfrak{I}$-holomorph of G. Then:*

(i) *if A is the associator of G, $(\mathfrak{I}, A)$ is that of E;*

(ii) *if A_2 is the centre of G/A, the Moufang nucleus of E is $(\mathfrak{I}, A_2)$;*

(iii) *the centre and the Moufang centre of E coincide, both being $(1, Z)$, where 1 is the unit of $\mathfrak{I}$, Z the centre of G;*

(iv) *if G is associatrally nilpotent of class n so is E; and conversely;*

(v) *E is Moufang nilpotent if and only if it is associatrally nilpotent; if it has associatral class n it has Moufang class $[(n+1)/2]$ (the greatest integer not exceeding $(n+1)/2$).*

Corollary. *If G (and hence E) is associatrally nilpotent of class 2, E is Moufang, and the inner mapping group of E is a group of automorphisms.*

Remark. If we start with a commutative Moufang loop G, centrally nilpotent of class 2, we see from (i), (iii), and the corollary that E is a non-commutative Moufang loop whose inner mapping group is a group of automorphisms.

Proof. By Theorem 7A (iv) of Chapter II, a necessary and sufficient condition that the inner mapping group of a Moufang loop G be a group of automorphisms is that G/A (where A is the associator of G) be a commutative Moufang loop in which every element save the identity has order three. We proceed to the proof of Theorem 5C.

(i) This follows from Theorem 5A(ii).

(ii) Since A_2 is precisely the set of all elements x of the Moufang loop G such that xUL_x^{-1} is in A for every U of $\mathfrak{I}$, this is a consequence of Theorem 5A(v).

(iii) Now $uS=u$ for every S of $\mathfrak{I}$ if and only if u is in the centre Z of G. If further U is an element of $\mathfrak{I}$ such that $xU=uxu^{-1}=x$ for all x of G, then $U=1$. Thus, by Theorem 5A(vi), the Moufang centre of E is $(1, Z)$. Since $Z\leqq A$, the intersection of the associator $(\mathfrak{I}, A)$ and the Moufang centre $(1, Z)$ of E is $(1, Z)$, which is therefore also the centre of E.

(iv) If $\mathfrak{K}$ is the set of all S of $\mathfrak{I}$ such that xSL_x^{-1} is in A, it is readily verified that the inner mapping group of the commutative Moufang loop G/A is isomorphic to $\mathfrak{I}/\mathfrak{K}$. But, by Theorem 5B (iii), $(\mathfrak{I}, G)/(\mathfrak{K}, A)$ is isomorphic to $(\mathfrak{J}/\mathfrak{K}, G/A)$, the latter being the $(\mathfrak{J}/\mathfrak{K})$-holomorph of G/A. Now (iv) is certainly true for $n=0$. But, if we assume inductively that (ii) is true for some $n-1\geqq 0$, then, since G/A is associatrally nilpotent of class $n-1$, so is $(\mathfrak{J}/\mathfrak{K}, G/A)$; and it follows that $(\mathfrak{J}, G)$ is associatrally nilpotent of class n. This completes the proof of (iv).

(v) If $\mathfrak{L}$ is the set of all S of $\mathfrak{J}$ such that xSL_x^{-1} is in A_2, it follows that (in the sense of isomorphism) $\mathfrak{J}/\mathfrak{L}$ is the inner mapping group of G/A_2. Moreover $(\mathfrak{J}, G)/(\mathfrak{L}, A_2)$ is isomorphic to $(\mathfrak{J}/\mathfrak{L}, G/A_2)$, the $(\mathfrak{J}/\mathfrak{L})$-holomorph of G/A_2. Thus the proof proceeds as before. If G is associatrally nilpotent of class $n=0$, $n=1$ or $n=2$, then E is Moufang nilpotent of class $[(n+1)/2]$, since it is in these cases, respectively, a group of order one, a group of order greater than one (by (i)), or a non-associative Moufang loop (by (i) and (ii)). If G is associatrally nilpotent of class $n>2$, then G/A_2 is associatrally nilpotent of class $n-2$; and we assume inductively that $(\mathfrak{J}/\mathfrak{L}; G/A_2)$ is Moufang nilpotent of class $[(n-1)/2]$. But then $(\mathfrak{J}, G)$ is Moufang nilpotent of class $1+[(n-1)/2]=[(n+1)/2]$. This completes the proof of (v).

As to the corollary, if G is associatrally nilpotent of class 2, G/A is an abelian group (since in any case it is a commutative Moufang loop) and thus xUL_x^{-1} is in A for every U of $\mathfrak{J}$. Thus $((\mathfrak{J}, G)/\mathfrak{J}, A)$ is isomorphic to the abelian group G/A. Since $(\mathfrak{J}, A)$ is the associator of the Moufang loop $(\mathfrak{J}, G)$, and since every element of G/A save the identity has order 3, the inner mapping group of $E=(\mathfrak{J}, G)$ is a group of automorphisms.

We may deduce from the last two theorems another example of the fact that characteristic subloops need not be normal.

THEOREM 5D. *There exists an I.P. loop whose associator is not a normal subloop.*

Proof. Let G be a commutative Moufang loop, centrally nilpotent of class 3. (See Corollary 2 to Theorem 8H, Chapter II.) By Theorem 5A(ii), $E=(\mathfrak{J}, G)$ has associator $(\mathfrak{J}, Z)$. Now $A_2\equiv Z_2$, the set of all x of G such that xUL_x^{-1} is in $A\equiv Z$ for all U of $\mathfrak{J}$, is a proper subloop of G, and hence, by Theorem 5B(i), $(\mathfrak{J}, Z)$ is not a normal subloop of E.

6. **Commutative loops expressible in terms of Moufang loops.** If G and G_0 are two groupoids with the same elements (see §1 of Chapter I), and if the product xoy can be expressed in terms of the elements x, y, the operation $(\cdot)$ of G, and any fixed mappings of the set G into itself, we shall say that G_0 is *expressible* in terms of G. When defined in these vague terms, the notion of expressibility seems altogether too general to be of any use. It is to be noted that expressibility contains isotopy as a special case, but is not however an equivalence relation. We shall be content here to consider the case that G is a group or a Moufang loop, and to investigate certain special situations where G_0 turns out to be a commutative loop.

A concept of expressibility, sufficiently restricted to be useful, has been enunciated for linear algebras by R. W. Wagner (Bull. Amer. Math. Soc. Abstract 48-5-168). However, Wagner's work has not yet been published.

In Chapter II (§8) we considered a Moufang loop G for which the mapping $x\rightarrow x^3$ was an endomorphism into its centre, and showed in particular that the system G_0, with multiplication given by $xoy=x^{-1}yx^2$, was a commutative Moufang loop. This then is our first nontrivial example of an expressibility relation.

As a generalization, let G be a Moufang loop, let $m=2n+1$ be a fixed odd positive integer, and assume that the mapping $x\rightarrow x^m$ is an endomorphism of G into its centre. Then $(x^{-1}y)^m=(x^{-1}y)^n x^{-1}y(x^{-1}y)^n=x^{-m}y^m$, and so $(x^{-1}y)^n x^{2n}=(y^{-1}x)^n y^{2n}$. Therefore, under this assumption, the system G_*, expressed in terms of G by the relation

$$(6.1) \qquad x*y = (x^{-1}y)^n x^{2n},$$

is a commutative groupoid. (It should be noted that the above trick fails when m is an even integer.)

It will not be true in all cases that G_* is a quasigroup. In fact, if x, z are given elements, and if we seek an element y of G such that $x*y=z$, we arrive immediately at the equation $(x^{-1}y)^n=zx^{-2n}$. Clearly the latter equation will determine y uniquely in all cases if and only if the mapping $x\rightarrow x^n$ is a one-to-one mapping of G upon G. Suppose that this condition is verified, so that the mapping T defined by $xT=x^n$ possesses a (unique) inverse T^{-1}. Then G_* is a quasigroup. Moreover we have $x*1=1*x=x^n=xT$. Thus the system G_0, defined by

$$(6.2) \qquad xoy = (xT^{-1})*(yT^{-1}), \qquad xT = x^n,$$

will be a commutative loop with unit 1.

In the situation of Chapter II we had $m=3$, $n=1$; and so T was the identity mapping. As a more general case we may assume the existence of a fixed integer k such that $xT^{-1}=x^{-k}$ for all x, and hence $x=(xT^{-1})T=x^{-kn}$, $x^{kn+1}=1$. Now if n is greater than 1, there exists no integer k such that $kn+1=0$. Hence, in the case $n>1$, the last assumption requires that every element x of G should generate a finite group. We are thus led to the consideration of Moufang loops in which every element has bounded positive order.

Rather than treat all of the possibilities in their utmost generality, let us consider a Moufang loop G in which every element x generates a finite group. Then to each $x\neq 1$ there will correspond a positive integer p (the order of x) such that $x^p=1$ but $x^q\neq 1$ for $0<q<p$. We shall assume that the various orders p are bounded odd integers. Then the least common multiple m of these orders will exist and be odd: $m=2n+1$. Moreover we shall have $x^m=1$ for every x. It is thus apparent that the following lemma applies to a large variety of Moufang loops (and thus to groups), all of whose elements are of finite bounded odd order. In particular the lemma will hold for finite Moufang

loops without elements of even order.

LEMMA 6A. *Let n be a positive integer, and let G be a Moufang loop in which $x^{2n+1}=1$ for every x. Then the groupoid G_0, defined by*

$$xoy = (x^2y^{-2})^nx^2, \tag{6.3}$$

is a commutative loop with unit 1.

Proof. $1=(x^2y^{-2})^{2n+1}=(x^2y^{-2})^nx^2y^{-2}(x^2y^{-2})^n=(xoy)(yox)^{-1}$, and so $yox=xoy$ for all x, y of G. Further, if $xoy=z$ where x, z are given, then $(x^2y^{-2})^n=zx^{-2}$, and so $(xz^{-2})^{-2}=x^2y^2$, $y^{-2}=(zx^{-2})^{-2}x^{-2}$, $y=y^{-2n}=[(zx^{-2})^{-2}x^{-2}]^n$. Finally, $1ox=xo1=x^{2n+2}=x$. This completes the proof.

THEOREM 6A. *A necessary and sufficient condition that the commutative loop G_0 defined in Lemma* 6A *should have the inverse property is that*

$$x\cdot y^{-1}xy = y^{-1}xy\cdot x \tag{6.4}$$

for all x, y of the Moufang loop G. When (6.4) *holds true, G_0 may be defined alternatively by*

$$xoy = (xy^2x)^{-n}; \tag{6.5}$$

that is to say, the equation

$$(x^2y^{-2})^nx^2 = (xy^2x)^{-n} \tag{6.6}$$

holds for all x, y of G.

Proof. If $xoy=(x^2y^{-2})^nx^2=1$ then $(x^2y^{-2})^n=x^{-2}$, $x^2y^{-2}=x^4$, $y^{-2}=x^2$ and $y=y^{-2n}=x^{2n}=x^{-1}$. Hence if G_0 has the inverse property, the inverse of x must be x^{-1}. It follows that the commutative loop G_0 has the inverse property if and only if $(xoy)oy^{-1}=x$ for all x, y. But $(xoy)oy^{-1}=y^{-1}o(xoy)=[y^{-2}(xoy)^{-2}]^ny^{-2}$. Hence G_0 has the inverse property if and only if $[y^{-2}(xoy)^{-2}]^n=xy^2$ for all x, y. We may solve this equation for xoy in the form (6.5). In fact $[y^{-2}(xoy)^{-2}]^{-1}=(xy^2)^2$, $(xoy)^2y^2=xy^2xy^2$, $(xoy)^2=xy^2x$, and $xoy=(xy^2x)^{-n}$. Moreover each step is reversible, so that G_0 has the inverse property if and only if (6.3) and (6.5) are equivalent; that is to say, if and only if (6.6) holds for all x, y of G.

From (6.5) and the fact that G_0 is commutative we derive $(xy^2x)^{-n}=xoy=yox=(yx^2y)^{-n}$, whence

$$xy^2x = yx^2y \tag{6.7}$$

for all x, y. If we replace x by xy^{-1} in (6.7) we obtain $x\cdot yxy^{-1}=yxy^{-1}\cdot x$, which is equivalent to (6.4). Conversely, from (6.4) with x replaced by xy^{-1} there results $xy^{-2}x=y^{-1}x^2y^{-1}$, which is equivalent to (6.7).

The proof will therefore be complete when we show that (6.7) (along with the assumption that $x^{2n+1}=1$ for every x of G) implies (6.6). It is simplest to proceed as follows. If xoy is given by (6.5) we have $1ox=xo1=x$.

Moreover $xoy=yox$ by (6.7). Thus $(xoy)oy^{-1}=(yox)oy^{-1}=[y^{-1}(yox)^2y^{-1}]^{-n}$ $=(y^{-1}\cdot yx^2y\cdot y^{-1})^{-n}=x^{-2n}=x$, and so G_0, when defined by (6.4), (6.5), is a commutative I.P. loop. Now from (6.5), $yox^{-1}=(yx^{-2}y)^{-n}$, $(yox^{-1})^2=yx^{-2}y$, $(yox^{-1})^2x^{-2}=(yx^{-2})^2$, $x^2(yox^{-1})^{-2}=(yx^{-2})^{-2}$, and

$$[x^2(yox^{-1})^{-2}]^nx^2 = yx^{-2}\cdot x^2 = y. \tag{6.8}$$

Now in (6.8) replace y by yox, and we derive $(x^2y^{-2})^nx^2=yox=xoy=(xy^2x)^{-n}$, or (6.6).

If G_0 is defined as in Lemma 6A it is clear that to any subloop H of G there corresponds a subloop H_0 of G_0, consisting of the same elements. Moreover, it is not too difficult to show that if H is normal in G then H_0 is normal in G_0, and G_0/H_0 may be obtained from G/H just as G_0 is obtained from G. (This last would be false in some cases if we had assumed that $2n+1$ was the *least* common multiple of the orders of the elements of G; but we have in fact made no such assumption.)

When G is a group, equation (6.4) may be expressed by saying that *every two conjugate elements of the group G commute* (or *are permutable*). Such groups G have been considered by Burnside [1], with particular reference to the case that G has a finite number of generators. Burnside's paper is not wholly free from error—the part dealing with the possible orders is based on earlier incorrect results which were later corrected by others (Levi-van der Waerden [1])—but we shall state in the form of a lemma certain of the correct results which we shall use. (For further details, see Theorem 6C below.)

LEMMA 6B. *Let G be a group in which every two conjugate elements commute, and let* $(x, y)=x^{-1}y^{-1}xy$, $(x, y, z)=((x, y), z)$, *and generally* $(x_1, x_2, \cdots, x_k)$ $=((x_1, x_2, \cdots, x_{k-1}), x_k)$, *denote the usual commutators. Then*:

(i) $(x^r, y^s)=(x, y)^{rs}$ *for all x, y of G and for all integers r, s*;

(ii) $(x, y, z)^3=1$ *for all x, y, z*;

(iii) *interchange of any two of the elements* x_i *in a commutator* $(x_1, x_2, \cdots, x_k)$ *replaces the commutator by its inverse*;

(iv) *if G has a finite number of generators, each of finite order, the order of G is finite*;

(v) *if every element of G has finite odd order, the elements of order prime to 3 form a subgroup P which is nilpotent of class at most two*; *the elements of order a power of 3 form a subgroup Q*; *and G is the direct product* $P\times Q$.

Proof. For the proof of the first four statements see Burnside [1]. However (iv) is a direct consequence of (i), (ii) and (iii). As to (v), it follows from (iii) that (x, y) commutes with x and y, and hence we may show inductively that $(xy)^k=(x, y)^{km}x^ky^k$ where $m=(k-1)/2$. If k is the least common multiple of the orders of x and y, so that k is odd and m is an integer, we have $(xy)^k=(x, y^k)^m=1$. By considering the cases that k is prime to 3 and that k is a power of 3 we derive the existence of the groups P and Q. If x, y, z are in P,

$(x, y, z)=1$, by (ii); and hence P is nilpotent of class at most two. Again if x is in Q, and has order r, it follows from (i) that $(x, y^r)=(x^r, y)=1$. Hence every element y of P commutes with every element x of Q. This completes the essentials of the proof.

These groups, in fact, form a special case of the *regular* groups of P. Hall [1].

THEOREM 6B. *Let G be a group in which every two conjugate elements commute, and suppose that $x^{2n+1}=1$ for every element x of G, where n is a fixed positive integer. Then the groupoid G_0, consisting of the same elements as G under the multiplication G_0, is a commutative Moufang loop, centrally nilpotent of class at most 2. More specifically:*

(i) *$xoy=(x, y)^n\cdot xy$ for all x, y of G;*

(ii) *the centre of G_0 consists of the elements of Z_2, where Z and Z_2/Z are the centres of G and G/Z respectively;*

(iii) *the derived loop of G_0 is $(G', G)=(G, G, G)$; in fact we have $[x, y, z]=(x, y, z)^n$, where the first symbol has been defined in* §9 *of Chapter* II;

(iv) *G_0 is centrally nilpotent of class at most* 2.

Proof. That G_0 is a commutative I.P. loop follows from Theorem 6A. We shall defer for the moment the proof that G_0 is Moufang, and take up the other points in order.

(i) Now $xoy=(xy^2x)^{-n}$. But, by Lemma 6B, $yx=(y^{-1}, x^{-1})xy=(x, y)^{-1}xy$; $xy^2x=(x,y)^{-1}(xy)^2$, since (x,y) commutes with x and y; and $xoy=(x,y)^n(xy)^{-2n}=(x, y)^nxy$.

(ii) The element c is in the centre of the commutative loop G if and only if $co(yox)=yo(cox)$ for all x, y. Using the form $xoy=(xy^2x)^{-n}$ we derive the equivalent equation $c\cdot yx^2y\cdot c=y\cdot cx^2c\cdot y$, or, on replacing x by x^{-n}, and rearranging,

$$(c, y)x = x(c^{-1}, y^{-1}) \tag{6.9}$$

for all x, y. Now $(c^{-1}, y^{-1})=(c, y)$ by Lemma 6B(i); and hence c is in the centre of G_0 if and only if (c, y) is in Z for all y. This is equivalent to stating that c is in Z_2.

(iii) If u is the solution of the equation $(xoy)oz=uo(yoz)$, the element $x^{-1}ou$ is the derived loop of the commutative loop G_0; and, conversely, the derived loop is generated by the set of all elements $x^{-1}ou$. The equation for u may be rewritten in the form $zo(yox)=(yoz)ou$, and this is equivalent to $z\cdot yx^2y\cdot z=(yoz)u^2(yoz)$, or to

$$u^2 = (yoz)^{-1}zy\cdot x^2\cdot yz(yoz)^{-1}. \tag{6.10}$$

We simplify this by use of Theorem 6B (i). In fact $(yoz)^{-1}zy=(y, z)^{-n}z^{-1}y^{-1}\cdot zy=(y, z)^{-n}(z, y)=(y, z)^{-n-1}=(y, z)^n$, and likewise $yz(yoz)^{-1}=yz\cdot z^{-1}y^{-1}(y, z)^{-n}=(y, z)^{-n}$. Hence we have $u^2=(y, z)^nx^2(y, z)^{-n}=((y, z)^{-n}, x^{-2})x^2=(y, z, x)^{2n}x^2$

$=(x, y, z)^{-1}x^2$. Now (x, y, z) is commutative with x, by Lemma 6B (iii), and hence $u=(u^2)^{-n}=x\cdot(x, y, z)^n$. Again, $x^{-1}ou=(x^{-1}, u)^n x^{-1}u=(x, u)^{-n}(x, y, z)^n$. But $(x, u)=(u, x)^{-1}=(x, y, z, x)^{-n}=1$, and hence $x^{-1}oy=(x, y, z)^n$. It follows that the derived loop of G_0 is generated by the $(x, y, z)^n$ and hence by the (x, y, z). In particular, then, the derived loop consists of the same elements as $(G', G)=(G, G, G)$. We also note that $[x, y, z]\equiv x^{-1}o\{[(xoy)oz]o(yoz)^{-1}\}$ $=x^{-1}ou=(x, y, z)^n$.

(iv) If x, y, z, u, v are any five elements of G_0 we have $[[x, y, z], u, v]$ $=((x, y, z)^n, u, v)^n=(x, y, z, u, v)^k$, where $k=n^2$. It follows that the symbol $[[x, y, z], u, v]$ has the "skew-symmetry" of (x, y, z, u, v). If G_0 is a commutative Moufang loop, we have that G_0 is nilpotent of class at most 2, by authority of Lemma 9B (Chapter II).

Finally we must prove that G_0 is Moufang. Now $[(xoy)\circ(xoz)]^2$ $=(xoy)xz^2x(xoy)$. But, by (i) of the present theorem, $(xoy)x=(x, y)^n xyx=$ $(x, y)^n x(y^{-1}, x^{-1})xy=(x, y)^{n-1}x^2y$, and $x(xoy)=(x, y)^n x^2y=(x, y)^n(x^{-2}, y^{-1})yx^2$ $=(x, y)^{n+2}yx^2=(x, y)^{-n+1}yx^2$. Thus $[(xoy)o(xoz)]^2=x^2y\cdot(x, y)^{n-1}z^2(x, y)^{-n+1}$ $\cdot yx^2=x^2y\cdot(x, y, z)^{2n-2}z^2yx^2$. However $(x, y, z)^{2n-2}=(x, y, z)^3=1$, by Lemma 6B(ii), and thus $[(xoy)o(xoz)]^2=x^2\cdot yz^2y\cdot x^2=x^2(yoz)^2x^2=[x^2o(yoz)]^2$. But $xox=(x, x)^n x^2=x^2$, by (i) again, and so $(xoy)a(xoz)=(xox)o(yoz)$ for all x, y, z of G_0. Therefore G_0 is a commutative Moufang loop, and the proof of Theorem 6B is complete.

We may now use Theorem 6B to make more precise the results of Burnside.

THEOREM 6C. *If G is a group in which every two conjugate elements commute, and if every element of G has finite, bounded, odd order, G is nilpotent of class at most* 4.

Proof. Under the above hypotheses there must exist an odd integer $2n+1$ such that $x^{2n+1}=1$ for every n. Let $1=Z_0<Z_1<Z_2<Z_3<\cdots$ be the upper central series of G. By Theorem 6B, since G_0, with centre and derived loop consisting of the elements of Z_2 and of (G', G) respectively, is centrally nilpotent of class at most 2, we must have $(G', G)\leqq Z_2$. But then the usual proof shows that $G'=(G, G)\leqq Z_3$ and that $G\leqq Z_4$. Hence G is nilpotent of class at most 4.

In view of the case where all the elements of G have order 3, we know that class 3 is attainable. It is, so far as I know, an open question as to whether there also exist such groups of class 4.

7. **Structure theorems for totally symmetric quasigroups.** A quasigroup G is said to be *totally symmetric* (or a T.S. quasigroup) if and only if every valid equation $xy=z$ in G remains true under all permutations of x, y and z. In other words, a T.S. quasigroup G is characterized by the laws

$$xy = yx, \qquad x\cdot xy = y. \tag{7.1}$$

In Bruck [1] methods were given for constructing a wide variety of T.S. quasigroups, and the isotopy properties of such quasigroups and loops were studied to a considerable extent. In Bruck [2], T.S. loops were used for the construction of certain types of simple algebra. As will be seen in what follows, we may amplify the theory of T.S. quasigroups considerably, and quite effortlessly, by studying the structure of the autotopism group (compare Chapter I, §11 and Chapter II, §4).

LEMMA 7A. *If the triple* (U, V, W) *is an autotopism of the totally symmetric quasigroup* G, *so are the other five triples obtainable by permutation of* U, V *and* W.

Proof. The proof parallels closely the proof of Lemma 4A of Chapter II. By hypothesis, U, V, W are one-to-one mappings of G upon itself, and

$$xU\cdot yV = (xy)W \tag{7.2}$$

for all x, y of G. Since G is commutative, interchange of x and y in (7.2) shows that (V, U, W) is also an autotopism. Since $xy\cdot y=y\cdot yx=x$ for all x, y, we may replace x by xy in (7.2) and derive $(xy)U\cdot yV=xW$, and thus $xW\cdot yV=(xy)U$. Hence (W, V, U) is an autotopism. The rest of the lemma is an immediate consequence of these two facts.

LEMMA 7B. *If* U, W *are one-to-one mappings of the T.S. quasigroup* G *upon itself, and if* I *is the identity mapping, necessary and sufficient conditions that the triple* (U, I, W) *be an autotopism are that* $W=U^{-1}$ *and that*

$$xU\cdot y = x\cdot yU \tag{7.3}$$

for all x, y *of* G.

COROLLARY. *The set* $\mathfrak{C}$, *consisting of all one-to-one mappings* U *of* G *upon itself which satisfy* (7.3), *is an abelian group.*

Proof. If (U, I, W) is an autotopism, we have

$$xU\cdot y = (xy)W \tag{7.4}$$

for all x, y of G. Interchange of x and y gives (7.3). Conversely if U is a one-to-one mapping of G upon itself, and if U satisfies (7.3), we replace y by yU^{-1} in (7.3) and have that (U, U^{-1}, I) is an autotopism. Thus, by Lemma 7B, (U, I, U^{-1}) is an autotopism. But if (U, I, W) is also an autotopism, so is $(U, I, W)(U, I, U^{-1})^{-1}=(I, I, WU)$. Hence $xy=(xy)WU$ for all x, y, or $WU=I$, $W=U^{-1}$. This completes the proof of Lemma 7A. As to the corollary, if (U, I, U^{-1}) is an autotopism, so is $(U, I, U^{-1})^{-1}=(U^{-1}, I, U)$; hence $\mathfrak{C}$ contains the inverse of each of its members. If V is also in $\mathfrak{C}$, $(U, I, U^{-1})(V, I, V^{-1})=(UV, I, U^{-1}V^{-1})$ is an autotopism. It follows from Lemma 7B both that UV is in $\mathfrak{C}$, so that $\mathfrak{C}$ is a group, and that $U^{-1}V^{-1}=(UV)^{-1}$, so that $VU=UV$, $\mathfrak{C}$ is an abelian group.

DEFINITION. A one-to-one mapping U of a T.S. quasigroup G upon itself will be called an *autotopic* mapping if and only if there exist two one-to-one mappings V, W of G upon itself such that (U, V, W) is an autotopism of G.

Note that, in view of Lemma 7A, V and W will also be autotopic mappings.

THEOREM 7A. *The set of all autotopic mappings U of a T.S. quasigroup G forms a group $\mathfrak{H}$. The group $\mathfrak{H}$ contains the group $\mathfrak{C}$, defined in the corollary to Lemma* 7B, *as a normal subgroup. Moreover*:

(i) *to every autotopic mapping U in $\mathfrak{H}$ there corresponds a uniquely defined mapping T in C such that (U, U, UT) is an autotopism of G*;

(ii) *every autotopism of G has the form (U, UR, US) where U is in H, R, S are in C, and where the mapping associated with U, in the sense of* (i), *is $T=RS$.*

Proof. If U is in $\mathfrak{H}$ there exist mappings V, W (also in $\mathfrak{H}$), such that (U, V, W) is an autotopism. But then $(U, V, W)^{-1}=(U^{-1}, V^{-1}, W^{-1})$ is an autotopism, so U^{-1} is in $\mathfrak{H}$. Moreover if U_1 is in $\mathfrak{H}$, (U_1, V_1, W_1) is an autotopism for some V_1, W_1, and hence $(U, V, W)(U_1, V_1, W_1)=(UU_1, VV_1, WW_1)$ is an autotopism, UU_1 is in $\mathfrak{H}$. Thus $\mathfrak{H}$ is a group. Since in addition $(U, V, W)^{-1}(S, I, S^{-1})(U, V, W)=(U^{-1}SU, I, W^{-1}S^{-1}W)$, it follows by Lemma 7B that $U^{-1}\mathfrak{C}U=\mathfrak{C}$ for every U of $\mathfrak{H}$. Hence $\mathfrak{C}$, which is obviously a subgroup of $\mathfrak{H}$, is also normal in $\mathfrak{H}$.

It will be convenient to prove (i) and (ii) together. If (U, V, W) is an autotopism, then, by Lemma 7A, so are $(U, W, V)^{-1}(V, W, U)=(U^{-1}V, I, V^{-1}U)$ and $(U, V, W)^{-1}(W, V, U)=(U^{-1}W, I, W^{-1}U)$. It follows from Lemma 7B that the mappings $U^{-1}V=R$ and $U^{-1}W=S$ are in $\mathfrak{C}$, and that $(U, V, W)=(U, UR, US)$. Since R is in $\mathfrak{C}$, (R, I, R^{-1}) is an autotopism, and thus, by Lemma 7A, so is $(U, UR, US)(I, R, R^{-1})^{-1}=(U, U, USR)$. Hence if $T=SR=RS$, so that T is in $\mathfrak{C}$, (U, U, UT) is an autotopism. If (U, U, UT_1) is also an autotopism, so is $(U, U, UT)^{-1}(U, U, UT_1)=(I, I, T^{-1}T_1)$; and therefore $T^{-1}T_1=I$, $T_1=T$. Hence T is uniquely determined by U, although R and S will not be. In fact if (U, U, UT) is an autotopism, if R is any element of $\mathfrak{C}$, and if $S=TR^{-1}$, then $(U, U, UT)(I, R, R^{-1})=(U, UR, US)$ is an autotopism. This completes the proof of Theorem 7A.

From Theorem 7A we may deduce an interesting corollary.

COROLLARY. *There exists an endomorphism θ of $\mathfrak{H}$ with the following properties*:

(i) *(U, U, U^θ) is an autotopism of G for every U of $\mathfrak{H}$*;

(ii) *$U^{-1}U^\theta$ is in $\mathfrak{C}$ for every U of $\mathfrak{H}$*;

(iii) *$U^\theta=U^{-2}$ if U is in $\mathfrak{C}$*;

(iv) *if $U^\theta=U^{-2}$, and if U^2 is in $\mathfrak{C}$, U is in $\mathfrak{C}$*;

(v) *$U^\theta=I$ if and only if U is in $\mathfrak{C}$ and $U^2=I$*;

(vi) *$U^\theta=U$ if and only if U is an automorphism of G.*

Proof. The existence of the single-valued mapping $U \rightarrow U^\theta$ follows from Theorem 7A. Moreover $(U, U, U^\theta)(V, V, V^\theta) = (UV, UV, U^\theta V^\theta)$, so $(UV)^\theta = U^\theta V^\theta$, by Theorem 7A. This proves (i), and (ii) follows from the fact that $U^\theta = UT$ where T is in $\mathfrak{C}$. As to (iii), if U is in $\mathfrak{C}$, $(U, I, U^{-1})(I, U, U^{-1}) = (U, U, U^{-2})$ is an autotopism, so $U^\theta = U^{-2}$. Conversely, if $U^\theta = U^{-2}$, where U^2 is in $\mathfrak{C}$, then $U^{-1}U^\theta = U^{-3}$ is in $\mathfrak{C}$, and so $U = U^3 \cdot U^{-2}$ is in $\mathfrak{C}$. This proves (iv). As to (v), if $U^\theta = I$, then $U^{-1} = U^{-1}U^\theta$ is in $\mathfrak{C}$, so $U^\theta = U^{-2} = I$; and the converse follows from (iv). Finally, (vi) is a direct consequence of the definition of an automorphism.

THEOREM 7B. *Let L be a commutative I.P. loop, and let $G = L_0$ be the T.S. quasigroup, isotopic to L, with multiplication given by*

$$xoy = x^{-1}y^{-1}. \tag{7.5}$$

Let the groups $\mathfrak{H}$ and $\mathfrak{C}$ have the same significance for G as in Theorem 7A. *Then*:

(i) *$\mathfrak{C}$ is isomorphic to the centre of L*;

(ii) *U is in $\mathfrak{H}$ if and only if $xU = xA \cdot u$ for all x, where A is an automorphism of L and u is in the Moufang center of L*;

(iii) *if the element U of $\mathfrak{H}$ is given as in* (ii), *(U, U, U^θ) is an autotopism of G if and only if $xU^\theta = xA \cdot u^{-2}$ for all x.*

Remarks. (i) A T.S. loop is simply an I.P. loop in which $x^{-1} = x$ for all x. Thus if L is a T.S. loop, G and L are identical. Hence the theorem gives a determination of $\mathfrak{H}$ and $\mathfrak{C}$ for all T.S. loops. In this case, however, the results could have been obtained directly from Theorem 4D of Chapter II.

(ii) Note that U is an automorphism of G if and only if $u^3 = 1$. Thus the automorphism group of G contains that of L, sometimes as a proper subgroup.

Proof of Theorem 7B. It was shown in Bruck [1] that G is a T.S. quasigroup, and also that, on the other hand, not every T.S. quasigroup is isotopic to an I.P. loop. Indeed if $xoy = x^{-1}y^{-1}$ it is clear that $xoy = yox$; but also $xo(xoy) = x^{-1}(x^{-1}y^{-1})^{-1} = x^{-1} \cdot xy = y$. Hence G is totally symmetric, as stated.

(i) If S in $\mathfrak{C}$, $(xS)oy = xo(yS)$, or, equivalently, $xS \cdot y = x \cdot yS$, for all x, y of L. Setting $y = 1$, we get $xS = x \cdot s$ where $1S = s$, and hence $xs \cdot y = x \cdot ys$ for all x, y. Since L is commutative, s is in the center of L. Conversely let $xS = xs$, where s is in the centre of L. Then $xS \cdot y = xs \cdot y = x \cdot ys = x \cdot yS$, and so $(xS)oy = xo(yS)$, S is in $\mathfrak{C}$. If also $xT = xt$, where t is in the centre of L, $x(ST) = (xS)T = xs \cdot t = x \cdot st$. Thus the mapping $S \rightarrow s = 1S$ is an isomorphism of $\mathfrak{C}$ upon the centre of L.

(ii) *and* (iii). By Theorem 7A, U is in $\mathfrak{H}$ if and only if (U, U, UT) is an autotopism of G for some T of $\mathfrak{C}$. By (i), we may assume that $xT = xt$ for some element t in the centre of L. Thus $(xU)o(yU) = (xoy)UT$ for all x, y if and only if $(xU)^{-1}(yU)^{-1} = (x^{-1}y^{-1})U \cdot t$ for all x, y. If we let J, as usual, be the mapping $xJ = x^{-1}$, it follows that (UJ, UJ, JUR_t) is an autotopism of L. We may now apply the results of Theorem 4D of Chapter II, which states that every autotopism of a commutative I.P. loop L has form $(BR_v, BR_vR_a, BR_v^2R_a)$, where B is an automorphism of L, v is in the Moufang centre of L, and a is in the centre of L. Thus we have $UJ=BR_v=BR_vR_a$, $JUR_t=BR_v^2R_a$. First we see that $a=1$ and that $U=BR_vJ$. Next we have $JBR_vJR_t=BR_v^2$, whence $R_v^{-1}R_t=R_v^2$, or $R_t=R_v^3$. Thus $t=1R_v^3=v^3$, which merely reflects the known fact that the cube of every element of the Moufang centre of L lies in the centre of L. If now we set $A=BJ$, $u=v^{-1}$, we have $U=AJR_vJ=AR_u$, and $t=u^{-3}$, $U^\theta=UR_t=AR_u^{-2}$. Thus $xU=xA\cdot u$ and $xU^\theta=xA\cdot u^{-2}$ where A is an automorphism of L and u a Moufang element of L. Conversely, for an arbitrary automorphism A and an arbitrary Moufang element u, we have $(xoy)U^\theta=(x^{-1}y^{-1})A\cdot u^{-2}=[(xA)^{-1}\cdot(yA)^{-1}]u^{-2}=(xA\cdot u)^{-1}\cdot(yA\cdot u)^{-1}=(xU)o(yU)$. This completes the proof of (ii) and (iii).

THEOREM 7C. *Let G be a T.S. quasigroup and let $\mathfrak{H}$, $\mathfrak{C}$ and θ have the same meanings as in Theorem* 7A *and its corollary. Further let G_0 be a principal isotope of G with multiplication given by*

$$xoy = xU\cdot yV. \tag{7.6}$$

Then:

(i) *necessary and sufficient conditions that G_0 have the right inverse property are that U be in $\mathfrak{H}$ and U^2 be in $\mathfrak{C}$. Moreover, when these conditions are satisfied, the right-inverse of x in G_0 is xR where $R=VU^2U^\theta V^{-1}$*;

(ii) *similarly, for the left inverse property, V must be in $\mathfrak{H}$, V^2 in $\mathfrak{C}$; and when these conditions are satisfied the left inverse of x in G_0 is xL where $L=UV^2V^\theta U^{-1}$*;

(iii) *necessary and sufficient conditions that G_0 be a T.S. quasigroup are that U and V be in $\mathfrak{C}$; and in this case we have $xoy=xS\cdot y=x\cdot yS$, where $S=UV$*;

(iv) *if U, V are in $\mathfrak{C}$, a necessary and sufficient condition that G_0 be isomorphic to G is that $UV=W^{-1}W^\theta$ for some W of $\mathfrak{H}$.*

Proof. (i) First we shall show the sufficiency of the conditions. If U is in $\mathfrak{H}$, (U, U^θ, U) is an autotopism of G; and if U^2 is in $\mathfrak{C}$, (U^{-2}, U^2, I) is also an autotopism. Thus when both conditions are satisfied $(U^{-2}, U^2, I)(U, U^\theta, U)=(U^{-1}, U^2U^\theta, U)$ is an autotopism, and hence $(xU\cdot yV)U=x\cdot yVU^2U^\theta=x\cdot yRV$, where $R=VU^2U^\theta V^{-1}$. In this case $(xoy)oyR=(x\cdot yRV)\cdot yRV=x$, for all x, y of G, which means that G_0 has the right inverse property.

Now suppose conversely that G_0 has the right inverse property, the right inverse of y being yR, where R is some one-to-one mapping of G upon itself. Then $(xoy)oyR=(xU\cdot yV)U\cdot yRV=x$ for all x, y. Thus $(xU\cdot yV)U=x\cdot yRV$ and so $(xy)U=xU^{-1}\cdot yW$ for all x, y, where $W=V^{-1}RV$. Therefore (U^{-1}, U, W) is an autotopism, U is in $\mathfrak{H}$, and $(U^{-1}, U, W)(U^{-1}, U^{-1}, U^{-\theta})=(U^{-2}, I, WU^{-\theta})$ is an autotopism, where $U^{-\theta}=(U^{-1})^\theta$. By Lemma 7B we now have $WU^{-\theta}=(U^{-2})^{-1}=U^2$, $W=U^2U^\theta$. Therefore, finally, $R=VWV^{-1}=VU^2U^\theta U^{-1}$.

(ii) This proof is completely analogous to that of (i).

(iii) A T.S. quasigroup is simply a quasigroup with the inverse property for which $L=R=I$. By (i), $R=I=VU^2U^\theta V^{-1}$ implies $U^\theta=U^{-2}$ with U^2 in $\mathfrak{C}$. But it then follows from (iv) of the corollary to Theorem 7A that U is in $\mathfrak{C}$. Conversely, if U is in $\mathfrak{C}$, $U^\theta=U^{-2}$ by (v) of the same corollary, and hence $R=I$. Similarly $L=I$ if and only if V is in $\mathfrak{C}$. Finally, if U, V are in $\mathfrak{C}$, $xU\cdot yV=x\cdot yVU=x\cdot yS=xS\cdot y$, where $S=VU=UV$. (This follows most directly from (7.3).)

(iv) We may suppose that $xoy=x\cdot yS$ where $S=UV$ is in $\mathfrak{C}$. Now G_0 is isomorphic to G if and only if there exists a one-to-one mapping W of G_0 upon G (and hence, in this case, of G upon G) such that $(xW)o(yW)=(xy)W$, or $xW\cdot yWS=(xy)W$. But this holds if and only if (W, WS, W) is an autotopism of G; in other words, if and only if W is in H and $WS=W^\theta$, $S=UV=W^{-1}W^\theta$.

Theorem 7C leads to some interesting results if we consider the case that G_0 is a loop. If we define R_y as usual by $xR_y=xy=yx$, it follows here that $xR_y^2=xy\cdot y=x$, so $R_y^2=I$ for all y, and hence $R_y^{-1}=R_y$. Thus G_0 is a loop if and only if $U=R_p$, $V=R_q$ for fixed elements p, q of G. Under what circumstances will G_0 have the right inverse property? Since $U^2=R_p^2=I$, the only condition to be satisfied is that R_p be in $\mathfrak{H}$, or that (R_p, R_p, R_pT) be an autotopism, where $T=R_p(R_p)^\theta$ is in $\mathfrak{C}$. But then $px\cdot py=(p\cdot xy)T=pT^{-1}\cdot xy$ for all x, y. Taking $x=p$ we get $p^2\cdot py=pT^{-1}\cdot py$ for all y, whence $p^2=pT^{-1}$. Since moreover $xR_pT=(px)T=pT^{-1}\cdot x=p^2x=xR_{p^2}$, we see that $R_pT=R_{p^2}$. Thus we may state a lemma.

LEMMA 7C. *If G is a T.S. quasigroup and p is a fixed element of G, a necessary and sufficient condition that R_p should be in $\mathfrak{H}$ is that $p^2\cdot xy=px\cdot py$ for all x, y of G. Moreover the set M of all elements p of this type is a subquasigroup of G.*

COROLLARY 1. *If G_0 is a loop, isotopic to G, defined by $xoy=px\cdot qy$ where p, q are fixed elements of G, then G_0 has the right inverse property (left inverse property) if and only if p (if q) is in M.*

COROLLARY 2. *G is isotopic to a Moufang loop if and only if $M=G$.*

Proof. The first statement of Lemma 7C has been proved above. As to the second, if p, q are in M we have $p^2\cdot(q^2\cdot xy)=p^2\cdot(qx\cdot qy)=(p\cdot qx)(p\cdot qy)$ $=[q^2(pq\cdot x)][q^2(pq\cdot y)]=(q^2)^2[(pq\cdot x)(pq\cdot y)]$, or

$$(7.7)\qquad p^2\cdot(q^2\cdot xy) = (q^2)^2[(pq\cdot x)(pq\cdot y)].$$

Again, we have $p^2\cdot(q^2\cdot xy)=(q^2)^2[(p^2\cdot q^2)(xy)]$; but $p^2\cdot q^2=pq\cdot pq=(pq)^2$, and so

$$(7.8)\qquad p^2\cdot(q^2\cdot xy) = (q^2)^2[(pq)^2(xy)].$$

It follows from (7.8), (7.7) that $(pq)^2\cdot xy=(pq\cdot x)(pq\cdot y)$ for all x, y. Hence

pq is in M. Inasmuch as G is totally symmetric, this completes the proof of Lemma 7C.

In this proof we have used the fact that p^2 is in M when p is. Now p is in M if and only if R_p is in $\mathfrak{H}$; but if R_p is in $\mathfrak{H}$, (R_p, R_p, R_{p^2}) is an autotopism, R_{p^2} is in $\mathfrak{H}$, p^2 is in M.

Corollary 1 is an immediate consequence of Theorem 7C and the present lemma. Corollary 2 follows from Corollary 1 and the fact that every loop isotopic to a Moufang loop is Moufang.

The subquasigroup M (of the T.S. quasigroup G) discussed in Lemma 7C, has close analogies with the Moufang centre of a commutative I.P. loop, as may readily be verified by combining Theorems 7C, 7B with Lemma 7C. The set N of idempotent elements of M forms a subquasigroup of M, since if $p=p^2$, $q=q^2$ are in N, then $(pq)^2=pq\cdot pq=p^2\cdot q^2=pq$. If $N=G$, we have the curious case of a self-distributive T.S. quasigroup: $x\cdot yz=xy\cdot xz$ for all x, y, z of G. That such a G exists may be seen by taking the loop L of Theorem 7B to be any commutative Moufang loop in which every element (save the identity) has order 3. Conversely, it may be shown that every loop isotopic to a self-distributive T.S. quasigroup is a Moufang loop in which every element has order 3. But a self-distributive T.S. quasigroup G will have T.S. isotopes which are not self-distributive. To see this, let L be a commutative Moufang loop in which $x^3=1$ for every x, let f be any fixed centre element of L, and define L_0 by $xoy=f\cdot x^{-1}y^{-1}$. Then L_0 is commutative, and therefore it is totally symmetric, since $(xoy)oy=f\cdot f^{-1}xy\cdot y^{-1}=x$. However $xox=f\cdot x^{-2}=fx$, and hence L_0 will be self-distributive if and only if $t=1$. The point is thus proved when we reflect that the T.S. quasigroups L_0 corresponding to different choices of f are all isotopic.

We now turn our thoughts in a different direction.

THEOREM 7D. *Let G be a T.S. quasigroup, and let $\mathfrak{C}$ be the group defined in the corollary to Lemma* 7B. *Further, let f be any fixed element of G, and let A_f be the set of all elements s of G such that*

$$(7.9) \qquad fx\cdot sy = sx\cdot fy$$

for all x, y of G. Then A_f forms an abelian group under the operation $sot=f\cdot st$, and the mapping $S\rightarrow s=fS$ yields an isomorphism of $\mathfrak{C}$ upon A_f. Moreover if g is any other fixed element of G the mapping $s\rightarrow f\cdot gs$ yields an isomorphism of A_f upon A_g.

Proof. Let S be any element of $\mathfrak{C}$, so that $xS\cdot y=x\cdot yS$ for all x, y of G. If we set $s=fS$, the last equation, with $x=f$, yields $s\cdot y=f\cdot yS$, or

$$(7.10) \qquad xS = f\cdot sx,$$

for all x of G. Suppose conversely that S is given in the form (7.10). Then S is in $\mathfrak{C}$ if and only if $(f\cdot sx)y=x\cdot(f\cdot sy)$ for all x, y of G. On replacing x, y by

sx, sy respectively, we derive the equivalent equation (7.9). We also note that if S is given by (7.10), $fS=f\cdot sf=s$.

Now suppose that T is also in $\mathfrak{C}$, and that $fT=t$. Then $f(ST)=f(TS)$ $=(fT)S=tS=f\cdot st$, by (7.10). Hence we have the correspondences $S\rightarrow s$, $T\rightarrow t$, $ST\rightarrow f\cdot st=sot$. Thus A_f is an abelian group, and the mapping $S\rightarrow s=fS$ is an isomorphism of $\mathfrak{C}$ on A_f. If g is any other fixed element of G, we note from (7.10) that $gS=f\cdot sg=f\cdot gs$. But the mapping $fS\rightarrow gS$, or $s\rightarrow f\cdot gs$, is evidently an isomorphism of A_f on A_g.

THEOREM 7E. *Let G be a T.S. quasigroup, and define $[x]$, for each fixed x, to be the set of all elements xS with S in $\mathfrak{C}$. Then the mapping $x\rightarrow[x]$ is a homomorphism of G upon a T.S. quasigroup $G/\mathfrak{C}$.*

Proof. It follows from the proof of Theorem 7D that $[f]$, for each f, consists of the same set of elements as the abelian group A_f. Thus the different "cosets" $[x]$ are in one-to-one correspondence. Moreover, if R, S, T are three elements of $\mathfrak{C}$, the equation $xR\cdot yS=zT$ is equivalent to the equation $(xy)R^{-1}S^{-1}=zT$. Thus it holds only if $[xy]=[z]$, and we may as well assume $z=xy$. In this case we have $(xy)R^{-1}S^{-1}=(xy)T$ or $RST=I$; and hence any two of R, S, T determine the third. We have proved that $[x]\cdot[y]=[xy]$, for all x, y. But then we see at once that the cosets $[x]$ form a T.S. quasigroup, say $G/\mathfrak{C}$, and that the mapping $x\rightarrow[x]$ is a homomorphism of G upon $G/\mathfrak{C}$.

A little reflection shows that the corresponding problem of construction should be solved as follows.

THEOREM 7F. *Let Q be a T.S. quasigroup, elements p, q, $\cdots$, and let A be an abelian group, elements S, T, $\cdots$. Let there be chosen, corresponding to every pair p, q of elements of G, an element $F_{p,q}$ of A with the properties that*

$$F_{p,q}=F_{q,p},\qquad F_{pq,q}=F_{p,q} \tag{7.11}$$

for all p, q of Q. Then the system $G=(Q,A)$, consisting of all couples (p,S) under the multiplication

$$(p,S)(q,T)=(pq,F_{p,q}S^{-1}T^{-1}), \tag{7.12}$$

is a T.S. quasigroup. Furthermore if A be represented as a group of one-to-one mappings of G upon G by use of the definition

$$(p,S)T=(p,ST), \tag{7.13}$$

then A is a subgroup of the abelian group $\mathfrak{C}$ defined in the corollary to Lemma 7B.

We omit the proof of Theorem 7F, which is perfectly straightforward. It should be noted, however, that *if we replace A by a commutative I.P. loop and pick the $F_{p,q}$ from its centre, G will still be a T.S. quasigroup.*

If the T.S. quasigroup G is a loop, $\mathfrak{C}$ is isomorphic with the centre of G, as follows from Theorem 7D with $f=1$. In any case $\mathfrak{C}$ has many of the properties of a centre (consider the "associative-commutative law" $xS\cdot y=x\cdot yS$), and the quotient quasigroup $G/\mathfrak{C}$ of Theorem 7E is a sort of "central" quotient. Moreover, by Theorem 7A, a necessary and sufficient condition that every autotopism (U, V, W) of G be an automorphism (in the sense that $U=V=W$) is that $\mathfrak{C}=I$. It follows from Theorem 7E that if G is finite we may, after formation of a finite number of successive "central" quotients, reach a T.S. quasigroup all of whose autotopisms are automorphisms. In order to give a nontrivial example of such a T.S. quasigroup we shall use the methods of Bruck [1] to construct a T.S. loop of order 3^n+1 whose centre has order 1, for every integer $n>1$.

Let G be an elementary abelian group of order 3^n, type (1^n), with $n\geqq 2$, and let G_0 be the T.S. quasigroup, isotopic to G, defined by $xoy=x^{-1}y^{-1}$. It follows from Theorem 7B (ii) that U is an autotopic mapping of G_0 if and only if $xU=xA\cdot u$ where A is an automorphism of G and u an element of G. By (iii) of the same theorem, every such U is an automorphism of G_0, since $u^{-2}=u$ and hence $U^\theta=U$. Moreover $xox=x^{-2}=x$ for all x of G. Now let G_* be the system of order 3^n+1 consisting of the elements of G with one additional element e, and let multiplication in G_* be defined as follows:

$$e*e = x*x = e; \qquad e*x = x*e = x;$$
$$x*y = xoy = x^{-1}y^{-1}; \tag{7.14}$$

where x, y are any two distinct elements of G. It was shown in Bruck [1], and it may also be verified directly, that G_* is a T.S. loop with unit e. If U is any one-to-one mapping of G upon G we may extend it to a one-to-one mapping of G_* upon G_* by defining $eU=e$. In this way we extend every automorphism U of G_0 to an automorphism of G_*, for we have $(eU)*(eU)=e*e=e=(e*e)U$, $(eU)*(xU)=e*(xU)=xU=(e*x)U$, $(xU)*(xU)=e=(x*x)U$, and $(xU)*(yU)=(xU)o(yU)=(xoy)U=(x*y)U$, where, as before, x and y are any two distinct elements of G. But if x and y are any two fixed elements of G it is clear that there exists an automorphism U of G_0 such that $xU=y$; we may in fact define U by $zU=z\cdot x^{-1}y$ for every z of G. Therefore the only characteristic subloops of G_* are the subloop of order one and G_* itself. Since $n\geqq 2$, G contains a subgroup H of order 9, and thus G_* contains a subloop H_* of order 10, consisting of e and the elements of H. Clearly H_* is not an abelian group (since, for example, all of its elements save e have order 2) and hence G_* is not an abelian group. Therefore the centre of G_* has order 1.

We also note that the ϕ-loop of G_* has order 1, and that the automorphism group of G_*, like that of G_0, has order $3^n(3^n-1)(3^n-3)\cdots(3^n-3^{n-1})$.

Bibliography

A. A. Albert

1. *Quasigroups.* I, Trans. Amer. Math. Soc. vol. 54 (1943) pp. 507–519.
2. *Quasigroups.* II, Trans. Amer. Math. Soc. vol. 55 (1944) pp. 401–419.

REINHOLD BAER

1. *Nets and groups*, Trans. Amer. Math. Soc. vol. 46 (1939) pp. 110–141.
2. *Nets and groups.* II, Trans. Amer. Math. Soc. vol. 47 (1940) pp. 435–439.
3. *The homomorphism theorems for loops*, Amer. J. Math. vol. 67 (1945) pp. 450–460.

G. BOL

1. *Geweben und Gruppen*, Math. Ann. vol. 114 (1937) pp. 414–431.

R. H. BRUCK

1. *Some results in the theory of quasigroups.* Trans. Amer. Math. Soc. vol. 55 (1944) pp. 19–52.
2. *Some results in the theory of linear non-associative algebras*, Trans. Amer. Math. Soc. vol. 56 (1944) pp. 769–781.
3. *Simple quasigroups*, Bull. Amer. Math. Soc. vol. 50 (1944) pp. 769–781.

W. BURNSIDE

1. *On groups in which every two conjugate elements are permutable*, Proc. London Math. Soc. vol. 35 (1902–1903) pp. 28–37.

HANS FITTING

1. *Beiträge zur Theorie der Gruppen endlicher Ordnung*, Jber. Deutschen Math. Verein. vol. 48 (1938) pp. 77–141.

G. N. GARRISON

1. *Quasi-groups*, Ann. of Math. vol. 41 (1940) pp. 474–487.

PHILIP HALL

1. *A contribution to the theory of groups of prime-power order*, Proc. London Math. Soc. (2) vol. 36 (1934) pp. 29–95.

B. A. HAUSMANN and OYSTEIN ORE

1. *Theory of quasi-groups*, Amer. J. Math. vol. 59 (1937) pp. 983–1004.

F. LEVI and B. L. VAN DER WAERDEN

1. *Über eine besondere Klasse von Gruppen*, Abh. Math. Sem. Hansischen Univ. vol. 9 (1933) pp. 154–158.

G. A. MILLER, H. F. BLICHFELDT and L. E. DICKSON

1. *Finite groups*, New York, 1916.

RUTH MOUFANG

1. *Zur Struktur von Alternativkorpern*, Math. Ann. vol. 110 (1935) pp. 416–430.

B. NEUMANN

1. *Some remarks on infinite groups*, J. London Math. Soc. vol. 12 (1937) pp. 120–127.

A. R. RICHARDSON

1. *Groupoids and their automorphisms*, Proc. London Math. Soc. (2) vol. 48 (1943) pp. 83–111.

M. F. SMILEY

1. *An application of lattice theory to quasigroups*, Bull. Amer. Math. Soc. vol. 50 (1944) pp. 782–786.

H. ZASSENHAUS

1. *Lehrbuch der Gruppentheorie*, vol. 1, Hamburger Mathematischen Einzelschriften, no. 1, 1937.

UNIVERSITY OF WISCONSIN,
MADISON, WIS.