CROSSED-INVERSE AND RELATED LOOPS[1]

BY

R. ARTZY

Introduction. *Crossed-inverse* (C.I.) loops are loops in which the identity $xy \cdot x' = y$ holds for all x, y of the loop, x' being the right inverse of x. Such loops have already been studied [1; 2], and the results were useful in the study of neofields [6] and of geometrical subjects [3]. C.I. loops are special *automorphic-inverse* loops, that is, loops satisfying the identity $(xy)' = x'y'$, for all x, y in the loop.

The first section of this paper deals with isotopic C.I. loops, and they are proved to be also isomorphic. Then the autotopisms of C.I. loops are studied, and the main result of this part is the fact that the "companions" of all the autotopisms, i.e. the elements that correspond to the translation elements of the isotopisms, form a subloop which is commutative and Moufang. §2 of the paper gives a necessary condition for the existence of finite automorphic-inverse loops consisting only of the unit element and inverse-cycles [cf. 1] of the same length. The condition concerning the equal length of all inverse-cycles is necessary for the transitivity of the automorphism group of the loop [2] and hence for the possibility of considering the loop as the additive loop of a neoring. The third part deals with a method of constructing infinite automorphic-inverse loops satisfying also certain other identities.

The author is grateful to R. H. Bruck for fruitful discussions on the subject of this paper.

1.1. Definitions.

1.11. The biunique mapping which maps every element, c, of a loop $(G, \cdot)$ on its right inverse will be called J. Thus $c \cdot cJ = 1$, and $cJ^{-1} \cdot c = 1$. In automorphic-inverse loops J is an automorphism.

1.12. In the principal isotope of the loop G, with the new operation $(*)$ such that $ag * fb = ab$, for all a, b in G, the ordered pair (g, f) is called the pair of *translation elements* of the principal isotope.

1.2. Elementary properties of C.I. loops.

1.21. The identities $ab \cdot aJ = b$ and $a(b \cdot aJ) = b$ are equivalent.

Proof. If P and Q are biunique mappings of the loop onto itself, then $PQ = I$, the identity mapping, if and only if $QP = I$. Let $L(x)$ and $R(x)$ be,

Presented to the Society, December 28, 1956, under the title *Loops with identities*, and August 30, 1957, under the title *Cross-inverse loops*; received by the editors August 2, 1957.

(1) Supported in part by the Research Committee of the Graduate School of the University of Wisconsin from funds supplied by the W. A. R. F.

respectively, the usual denotations for left and right multiplication by x. Then $L(a)$ and $R(aJ)$ are biunique mappings of the loop onto itself, and $L(a)R(aJ)=I$ is equivalent to $R(aJ)L(a)=I$.

1.22. From the C.I. property follows the automorphic-inverse property, but the converse statement is not true.

Proof. For the first part see [1]. The second part is proven by the existence of easily constructed counter examples.

1.23. Isotopes of C.I. loops are not necessarily C.I.

EXAMPLE. The following C.I. loop, with translation elements 2 and 3, yields a principal isotope which is not C.I.

1	2	3	4	5
2	1	4	5	3
3	5	1	2	4
4	3	5	1	2
5	4	2	3	1

If we denote the J-automorphism of 1.11 in the principal isotope by J^*, we get, e.g., $(3*4)*3J^*=3$, instead of 4.

1.24. If in a C.I. loop G an element belongs to one of the (right, left or middle) nuclei, A_ρ, A_λ, A_μ, respectively, then it belong to the centre, Z.

Proof. Let $z\in A_\rho$, that is

$$a\cdot bz = ab\cdot z \qquad \text{all } a, b\in G. \tag{1}$$

Equation (1) implies, with $a=dJ^{-1}$ and $b=cd$,

$$\begin{aligned} dJ^{-1}(cd\cdot z) &= (dJ^{-1}\cdot cd)z, \\ dJ^{-1}(cd\cdot z) &= cz, \\ cd\cdot z &= cz\cdot d. \end{aligned} \tag{2}$$

Putting $c=1$ yields $dz=zd$, for all d in G. Using this, we get $z\cdot cd=zc\cdot d$, and hence $z\in A_\lambda$. Now apply (1) in (2), and, in view of $xz=zx$ for all x in G, we get $c\cdot dz=c\cdot zd=cz\cdot d$, and hence $z\in A_\mu$.

If $z\in A_\lambda$ is assumed, the proof of $xz=zx$, all x in G, and $z\in A_\rho$ and $z\in A_\mu$ is analogous.

Now let $z\in A_\mu$, that is $az\cdot b=a\cdot zb$ for all a and b in G. Put $a=zJ^{-1}\cdot cJ^{-1}$ and $b=dc$. We get

$$\begin{aligned} ((zJ^{-1}\cdot cJ^{-1})z)\cdot dc &= (zJ^{-1}\cdot cJ^{-1})(z\cdot dc), \\ d &= (zJ^{-1}\cdot cJ^{-1})(z\cdot dc). \end{aligned}$$

$d\cdot zc=z\cdot dc$, and since for $c=1$ we get $xz=zx$ for all x in G, this becomes $d\cdot cz=dc\cdot z$, and hence $z\in A_\rho$. In view of the first part of the proof, this means $z\in Z$.

1.3. Isotopic C. I. loops.

LEMMA 1. *If a principal isotope of a C.I. loop G is again a C.I. loop, and if the principal isotope has the translation elements g and f, then*

$$fa\cdot gb = fg\cdot ab = (f\cdot ab)g = f(g\cdot ab), \qquad \text{all } a, b \text{ in } G.$$

Proof. The C.I. property implies $R(x)^{-1}=L(xJ^{-1})$ and $L(x)^{-1}=R(xJ)$ for all x in G. The unit element of the principal isotope is fg. For the right inverse of c in the principal isotope, cJ^*, we have $c*cJ^*=fg$,

$$(gJ^{-1}\cdot c)(cJ^*\cdot fJ) = fg,$$

$$cJ^* = f((fg)(gJ^{-1}\cdot c)J) = f((fg)(g\cdot cJ)).$$

Thus $J^*=JL(g)L(fg)L(f)$. Now, if the principal isotope is C.I., we have $c*(d*cJ^*)=d$,

$$cL(gJ^{-1})\cdot(dL(gJ^{-1})\cdot cJL(g)L(fg)L(f)R(fJ))R(fJ) = d.$$

Now the C.I. property implies $L(f)R(fJ)=I$, the identity mapping. Thus

$$cL(gJ^{-1})\cdot(dL(gJ^{-1})\cdot cJL(g)L(fg))R(fJ) = d,$$

$$dL(gJ^{-1})\cdot(cJL(g)L(fg)) = (d\cdot cL(gJ^{-1})J)R(fJ)^{-1}, \tag{3}$$

$$= (d\cdot cJL(g))L(f).$$

Put $cJL(g)=ab$ and $d=bJ^{-1}$. Then we get

$$(gb)J^{-1}(fg\cdot ab) = f(bJ^{-1}\cdot ab) = fa,$$

$$fg\cdot ab = fa\cdot gb. \tag{4}$$

Equation (4) with $a=1$ and $b=e$ yields

$$fg\cdot e = f\cdot ge, \tag{5}$$

and by setting $b=1$ and $a=e$ in (4) we have

$$fg\cdot e = fe\cdot g. \tag{6}$$

Apply now identities (5) and (6), with ab in place of e, in (4).

$$fa\cdot gb = f(g\cdot ab) = (f\cdot ab)g. \tag{7}$$

LEMMA 2. *Under the assumptions of Lemma* 1, *the following relations hold*: (i) $fg=gf$, (ii) $gJ^2=g$, (iii) $fJ^2=f$.

Proof. Since the isotope is C.I., we have identically $(c*d)*cJ^*=d$, that is,

$$(cL(gJ^{-1})\cdot dR(fJ))L(gJ^{-1})\cdot cJL(g)L(fg)L(f)L(f)^{-1} = d.$$

Put $cJL(g)=a$ and $bJ^{-1}=d$; then this becomes $(aJ^{-1}\cdot bJ^{-1}R(fJ))L(gJ^{-1})\cdot aL(fg)=bJ^{-1}$, or, because of the automorphic-inverse property,

$$(a\cdot bR(fJ^2))L(g)\cdot aJL((fg)J) = b,$$

or

$$g(a(b\cdot fJ^2)) = (fg\cdot a)b. \tag{8}$$

With $a=b=1$ this becomes

$$g\cdot fJ^2 = fg. \tag{9}$$

Equation (3) for the case $g\cdot cJ=gJ$ and $g\cdot dJ=1$ becomes $fg\cdot gJ=f$, or

$$fg = gf. \tag{10}$$

Comparison of (9) and (10) yields $fJ^2=f$, and as a consequence, $fJ=fJ^{-1}$ $=f^{-1}$. Equation (8) becomes now $g(a\cdot bf)=(fg\cdot a)b$. With $b=g$ and $a=gJ^{-1}$ this becomes $g(gJ^{-1}\cdot fg)=(fg\cdot gJ^{-1})g$, and in view of (10), $gf=(fg\cdot gJ^{-1})g$ or $f=gf\cdot gJ^{-1}$. The C.I. property yields $f=gf\cdot gJ$; thus $gJ=gJ^{-1}=g^{-1}$, and hence $g=gJ^2$.

THEOREM 1. *Isotopic C.I. loops are isomorphic.*

Proof. We have from Lemma 1 the relation $fa\cdot gb=(ab)L(f)R(g)$. Now $fa=aL(f)R(g)R(g)^{-1}$, and $gb=(f\cdot bL(g))f^{-1}$, which, in view of the combined equalities (5) and (6), equals $(fb\cdot g)f^{-1}=bL(f)R(g)L(f)^{-1}$. Now call $L(f)R(g)$ $=T$. Then is $aT*bT=aTR(g)^{-1}\cdot bTL(f)^{-1}=(ab)T$, and T is an isomorphism as required. (The present form of this proof has been influenced by a private communication by Shmuel Schreiber.)

THEOREM 2. *A principal isotope of a C.I. loop is C.I. if and only if the identity $fa\cdot gb=fg\cdot ab$ holds in the loop, g and f being the translation elements of the principal isotope.*

Proof. The necessity follows from Lemma 1.

Put in (4) $b=dJ$ and $a=d\cdot cJL(g)$, so that $ab=cJL(g)$. Then $(d\cdot cJL(g))L(f)\cdot dJL(g)=cJL(g)L(fg)$, $d\cdot cJL(g)=(dL(gJ^{-1})\cdot cJL(g)L(fg))$ $R(fJ)$, $d=cL(gJ^{-1})\cdot(dL(gJ^{-1})\cdot cJL(g)L(fg))R(fJ)=c*(d*cJ^*)$, which implies the C.I. property for the isotope.

1.4. **Some useful identities.** In the following, g and f will always denote the translation elements of a principal isotope, and a, b, c, d will be arbitrary elements of a C.I. loop.

1.41. Put, with modifications implied by Lemma 2, in (3) $a=g^{-1}d$ and $b=g\cdot cJ$. We get then

$$a(fg\cdot b) = f(ag\cdot b), \tag{11}$$

and with $b=1$,

$$a\cdot fg = f\cdot ag. \tag{12}$$

1.42. Equality (4) yields the autotopism $(L(f), L(g), L(fg))$. Now (J, J, J) and (J^{-1}, J^{-1}, J^{-1}) are automorphisms and therefore also autotopisms. Hence

$$(J, J, J)(L(f), L(g), L(fg))^{-1}(J^{-1}, J^{-1}, J^{-1}) = (R(f), R(g), R(fg))$$

is another autotopism, and

$$af \cdot bg = ab \cdot fg. \tag{13}$$

With $b=1$ this becomes

$$af \cdot g = a \cdot fg. \tag{14}$$

Apply (14) to (13) and get

$$af \cdot bg = (ab \cdot f)g. \tag{15}$$

1.43. In (11) substitute $c = aJ \cdot gJ$ and $d = (g \cdot bf)J$, that is, $a = gJ \cdot cJ^{-1}$ and $b = (f \cdot dg)J^{-1}$. The result is $(gJ \cdot cJ^{-1})(fg \cdot (f \cdot dg)J^{-1}) = f(cJ^{-1}L(gJ)R(g) \cdot (f \cdot dg)J^{-1}) = f(c(f \cdot dg))J^{-1}$, and $gc \cdot (f^{-1}g^{-1} \cdot (f \cdot dg)) = fJ \cdot (c(f \cdot dg))$. We have from (4) $gc \cdot d = fJ \cdot (c(f \cdot dg))$ and $(gc \cdot d)f = c(f \cdot dg)$. Set here $c=1$ and then $d=1$, and apply the resulting identities to the equality itself. We get $(gc \cdot d)f = c(d \cdot fg)$, and with $d=1$,

$$gc \cdot f = c \cdot fg. \tag{16}$$

1.5. **Autotopisms of C.I. loops.** Equation (4) implies that

$$\tau = (L(f), L(g), L(fg))$$

is an autotopism if $ag*fb = ab$ determines a principal isotope with the C.I. property. Let (U, V, W) be any autotopism. Then $1U \cdot aV = aW$, and $aU \cdot 1V = aW$, for every loop element a, hence

$$V = WL(1U)^{-1} = WR(1UJ), \qquad U = WR(1V)^{-1} = WL(1VJ^{-1}). \tag{17}$$

The ordered pair $(1V, 1U)$ will be called the *companion couple* of the autotopism (U, V, W), $1V$ the *left companion*, $1U$ the *right companion*, $1V \cdot 1U$ the *companion product*. The autotopism τ has the companion couple (g, f). Thus the companion couple coincides with the translation elements of the principal isotope which led to the autotopism τ. The converse is also true:

THEOREM 3. *Every autotopism of a C.I. loop G determines uniquely a C.I. principal isotope with translation elements equal to the companions of the autotopism.*

Proof. If the autotopism is (U, V, W), let $1V = g$, $1U = f$. Then (17) becomes $V = WR(fJ)$, $U = WL(gJ^{-1})$, and hence $aWL(gJ^{-1}) \cdot bWR(fJ) = (ab)W$. From the C.I. property follows now $aWR(g)^{-1} \cdot bWL(f)^{-1} = (ab)W$, and we obtain the principal isotope with $aW*bW = (ab)W$ and $xg*fy = xy$, for all a, b, x, y in G.

THEOREM 4. *In a C.I. loop G the left companions, the right companions and the companion products of the autotopisms form respective subloops of G. These loops are identical to each other.*

Proof. Let (U, V, W) be an autotopism. We have $aU \cdot bV = (ab)W$, for all a, b in G, and hence $bV = (ab)W \cdot aUJ = (ab)W \cdot (aJ)J^{-1}UJ$. Thus

$$(W, J^{-1}UJ, V) \tag{18}$$

is another autotopism, and by repetition of the process, also

$$(V, J^{-1}WJ, J^{-1}UJ). \tag{19}$$

Another autotopism is

$$(V, J^{-1}WJ, J^{-1}UJ)^{-1}(W, J^{-1}UJ, V) = (V^{-1}W, J^{-1}W^{-1}UJ, J^{-1}U^{-1}JV) = \theta,$$

say. By substituting $a=1$ and $b=1$ in $aU \cdot bV = (ab)W$, we get, respectively, $V^{-1}W = L(1U)$ and $U^{-1}W = R(1V)$. Hence

$$\theta = (L(1U), J^{-1}R(1V)^{-1}J, J^{-1}UJV) = (L(1U), L(1V), J^{-1}UJV).$$

Thus $(1U \cdot a)(1V \cdot b) = (ab)J^{-1}UJV = (ab)S$, say. For the case $a=1$ we find $S = L(1V)L(1U)$. Hence $(1U \cdot a)(1V \cdot b) = 1U(1V \cdot ab)$. Now put $a = 1V$ and $b = cR(1VJ)$, then we get $(1U \cdot 1V)(1V \cdot cR(1VJ)) = 1U(1V \cdot cR(1VJ))$ and $(1U \cdot 1V)c = 1U(1V \cdot c)$. Applying this relation with $c = ab$, we get $(1U \cdot a) \cdot (1V \cdot b) = (1U \cdot 1V) \cdot ab$.

Now let (U_i, V_i, W_i), $i=1, 2$, be autotopisms, $1V_i = g_i$, $1U_i = f_i$. Then $(L(f_i), L(g_i), L(f_ig_i))$ are autotopisms. Their product is

$$(L(f_1)L(f_2), L(g_1)L(g_2), L(f_1g_1)L(f_2g_2)),$$

and since $1L(f_1)L(f_2) = f_2f_1$ and $1L(g_1)L(g_2) = g_2g_1$, also $(f_2f_1 \cdot a)(g_2g_1 \cdot b) = (f_2f_1 \cdot g_2g_1) \cdot ab$. Thus (f_2f_1, g_2g_1) is a companion couple. If (g, f) is a companion couple, then by the automorphic-inverse identity, also (gJ, fJ) is a companion couple. As a consequence of (18) and (19), the existence of the autotopism $(L(f), L(g), L(fg))$ implies the existence of the autotopisms $(L(fg), L(fJ), L(g))$ and $(L(g), L(fJ \cdot gJ), L(fJ))$. Therefore, if any element appears as left or right companion or as companion product, it appears also in the other two roles(2).

DEFINITION. The subloop consisting of all the companions of G is called the *companion nucleus* of G.

All the centre elements of G belong, of course, to the companion nucleus C, and the centre Z is a normal subloop of C. In the following, a fact about C/Z will be proved.

---

(2) The statement in Bull. Amer. Math. Soc. Abstract 63-6-621 that the companions form a normal subloop was erroneous.

THEOREM 5. *Every element of C, appearing as right or left companion or as companion product, determines the two other elements uniquely, up to multiplication by centre elements. If at least one element of the triple is a centre element, so are the rest.*

Proof. (i) Let (g, f), (w, fz) be two companion couples with equal companion products. Then $w=fg\cdot(fz)J=fg\cdot(fJ\cdot zJ)$. By (4) we have $w=g\cdot zJ$. Another couple is then $(w\cdot gJ,\ fz\cdot fJ)=(zJ,\ z)$. Since z is a companion, $zJ=z^{-1}$. Now $za\cdot z^{-1}b=ab$, and with $a=1$, $z\cdot z^{-1}b=b$. Because of $z^{-1}b\cdot z=b$, we have $z^{-1}b=bz^{-1}$, and therefore $zx=xz$ for all x in G. By (8), with the companion couple (z^{-1}, z), we get $z^{-1}(c\cdot dz)=cd$, and $c\cdot dz=cd\cdot z$. Hence z belongs to the centre.

(ii) Let (g, f) and (g, fz) be two companion couples. Then $(gg^{-1},\ fz\cdot fJ)=(1,\ z)$ is a companion couple, and $za\cdot b=z\cdot ab$. Thus z is a centre element. The same treatment applies, of course, to companion couples (g, f) and (gz, f).

(iii) Let z be in Z, (z, f) a companion couple. The equality $fa\cdot zb=fz\cdot ab$ implies $fa\cdot b=f\cdot ab$, and f and fz belong to Z. Let now (g, f) be a companion couple with fg in Z. Then $(1, fg)$ is another companion couple, and (i) implies $fg\cdot fJ=g\in Z$; also $(fg,\ 1)$ is a companion couple, and $g^{-1}\cdot fg=f\in Z$. This completes the proof.

A well known fact about commutative Moufang loops [cf. 4] follows readily from Theorem 5.

COROLLARY. *In commutative Moufang loops the cubes of all elements are in the centre.*

Proof. A commutative Moufang loop is C.I., and its companion nucleus is the whole loop since each element x satisfies the identity $xa\cdot xb=x^2\cdot ab$. In view of (18) and (19), from the autotopism $(L(x), L(x), L(x^2))$ other autotopisms $(L(x^2), L(xJ), L(x))$ and $(L(xJ), L(x^2), L(x))$ can be derived. Then, applying the method of the proof of Theorem 5, (i), on these two autotopisms and using the power associativity of Moufang loops, we get $x^2\cdot(x^{-1})^{-1}=x^3\in Z$.

R. H. Bruck mentions [4] three special types of autotopisms of I.P. loops. The corresponding types are here (i) (T, T, T) where T is an automorphism, (ii) $(L(f), L(g), L(fg))$ where (g, f) is a companion couple, (iii) $(R(z), I, R(z))$ where I is the identity mapping and z is a centre element. From each of these types additional autotopisms may be derived by means of (18) and (19). As in the case of commutative I.P. loops, which are special C.I. loops, we can prove the following theorem, thus generalizing the corresponding theorem [4, p. 300].

THEOREM 6. *The autotopism group of a C.I. loop is generated by the autotopisms of the three types mentioned above: every autotopism has the form $\alpha\beta\gamma$ where α, β, γ are autotopisms of the types* (i), (ii), (iii), *respectively.*

Proof. Let (U, V, W) be an autotopism, $1U=f$, $1V=g$. Then, by (17), $(U, V, W)=(WL(gJ), WR(fJ), W)$. Now put $WR(fJ\cdot gJ)=T$. Then, by (16), $WL(gJ)=WR(fJ\cdot gJ)L(f)$, and, by (14), $WR(fJ)=WR(fJ\cdot gJ)L(g)$. Thus

$$(U, V, W) = (TL(f), TL(g), TL(fg)). \tag{20}$$

Let now z be any centre element; then $L(f\cdot zJ)R(z)=L(f)$, and $L(fz^{-1}\cdot g)R(z)=L(fg)$. Hence

$$(U, V, W) = (TL(f\cdot zJ)R(z), TL(g), TL(fz^{-1}\cdot g)R(z)). \tag{21}$$

(U, V, W) and $(L(f), L(g), L(fg))$ are autotopisms, and so is (T, T, T) in view of (20), and T is an automorphism. Now $(L(f\cdot zJ), L(g), L(fz^{-1}\cdot g))$ is an autotopism because $(fz^{-1}\cdot a)(gb)=(fz^{-1}\cdot g)\cdot ab$ follows from (4) and from the fact that z lies in Z; (fz^{-1}, g) is the companion couple of this autotopism. Now (21) can be written in the form

$$(U, V, W) = (T, T, T)(L(f\cdot zJ), L(g), L(fz^{-1}\cdot g))(R(z), I, R(z)) = \alpha\beta\gamma.$$

REMARK. In §1.6 we shall prove that for the type (ii) of Theorem 6 always $f=g$. Thus the autotopism β is necessarily of the form $(L(x), L(x), L(x^2))$.

1.6. **Companion loops.** A loop fulfilling the requirements of the companion nucleus of a C.I. loop will be called a *companion loop*, A. We define it as a C.I. loop with the property that for every g in A there is an f in A determined uniquely to within multiplication by centre elements, such that $fy\cdot gz=fg\cdot yz$ for all y and z in A. If we define a mapping ϕ by $f=g\phi$, the companion couples are of the form $(x, x\phi)$, and in view of Theorem 4, ϕ is an automorphism of A/Z. Moreover $x\phi^2=(x\phi\cdot x)^{-1}$, and $x\phi^3=x$, for all x in A/Z; hence ϕ is of order 3 or 1.

LEMMA 3. *Every inner mapping of a companion loop is an automorphism.*

Proof. Since the mapping ϕ is defined only up to multiplication by centre elements it should be understood in the proofs of this lemma and of Theorem 7, that for each of the expressions $c\phi$ or $c\phi^{-1}$ any of the possible values may be chosen. But once chosen, it must be kept fixed. Furthermore the choice must be restricted so that $1\phi=1$ and $\phi\phi^{-1}=I$.

Let now, for certain $a_1, a_2, \cdots, a_n$ in A, $S=\prod_{i=1}^{n} V_i(a_i)$, where V_i is either L or R. Let $T=\prod_{i=1}^{n} W_i$, where $W_i=R(a_i\phi)R(a_i)$ in case $V_i=R$, and $W_i=L(a_i)L(a_i\phi)$ in case $V_i=L$. Then repeated application of (7) and (15) yields $x\phi^{-1}S\phi=(xy)T$, for all x and y in A. Now assume S to be an inner mapping, i.e. $1S=1$. Then $x=1$ yields $yS=yT$. Put now $y=1$, and get $x\phi^{-1}S\phi=xT$. Thus $S=\phi^{-1}S\phi=T$, and therefore $xS\cdot yS=(xy)S$. Thus S is an automorphism of A.

In the following lemma an associativity property of companion loops will be given.

LEMMA 4. *If a, b, c are fixed arbitrary elements of A/Z then $ab\cdot c=a\cdot bc$ implies $c\phi J\cdot ab=(c\phi J\cdot a)b$.*

Proof. Write $(c\phi J\cdot ab)\cdot c\phi$ instead of ab, and $(c\phi J\cdot a)\cdot c\phi$ instead of a. Then is $((c\phi J\cdot ab)\cdot c\phi)c=((c\phi J\cdot a)\cdot c\phi)\cdot bc$, which becomes, by (13) and (15),

$$(c\phi J\cdot ab)(c\phi\cdot c)=((c\phi J\cdot a)b)(c\phi\cdot c) \quad \text{and} \quad c\phi J\cdot ab=(c\phi J\cdot a)b.$$

We are now able to prove the main theorem. In the proof some steps are borrowed from [5].

THEOREM 7. *Every companion loop A is commutative and Moufang.*

Proof. Let, for fixed elements a and b, $S=L(ab)R(aJ)R(bJ)$. Then S is an inner mapping and, by Lemma 3, an automorphism. It leaves fixed all elements z for which $ab\cdot z=a\cdot bz$. The z's form a subloop H of A because $xS=x$, $yS=y$ imply $(xy)S=xy$; and $xS=x$, $y=xJ$ imply $x\cdot xJS=1S$ and hence $xJ=xJS$. Now a is in H because $ab\cdot aJ=a(b\cdot aJ)$. Furthermore $b\phi^{-1}$ is in H because $ab\cdot b\phi^{-1}=a(b\cdot b\phi^{-1})$ by (14). Thus also $a\cdot b\phi^{-1}$ is in H, which means $ab\cdot(a\cdot b\phi^{-1})=a(b(a\cdot b\phi^{-1}))$. Apply (13) to the left hand side and (12) to the right hand side, and get $a^2(b\cdot b\phi^{-1})=a(a(b\cdot b\phi^{-1}))$. But $b\cdot b\phi^{-1}=b\phi J$, and thus $a^2\cdot b\phi J=a(a\cdot b\phi J)$. Application of Lemma 4 to this equality yields $b\phi^2\cdot a^2=(b\phi^2\cdot a)a$. Now let K be the subloop consisting of all w with $(b\phi^2\cdot a)w=b\phi^2\cdot aw$. Then a lies in K, and so does aJ. Thus we have $(b\phi^2\cdot a)\cdot aJ=b\phi^2$. In view of the C.I. property a and $b\phi^2$ commute. But, since a and b were chosen arbitrarily the loop is commutative and therefore an I.P. loop. Now, using Lemma 4C of [4, p. 296], we see that the autotopism

$$(L(y),\ L(x),\ L(yx))$$

implies the identity $ya\cdot by=(y\cdot ab)y$, and y is a Moufang element. But, since in a companion loop every element can appear as right companion y, all its elements are Moufang elements, and the loop is Moufang.

COROLLARY 1. *One companion of an autotopism of a C.I. loop is equal to the product of the other companion and a centre element.*

COROLLARY 2. *In type* (ii) *of Theorem* 6, $f=g$.

2. **Restrictions on the order of certain finite loops.** In this part we are going to establish a necessary condition for finite automorphic-inverse loops to have a transitive automorphism group; their inverse-cycles are consequently [cf. 2] of the same length. As in [1], an inverse-cycle is defined as consisting of all aJ^k, $k=0,\ 1,\ \cdots,\ n-1$, if $aJ^n=a$.

THEOREM 8. *If an automorphic-inverse loop G consists only of the unit element and r inverse-cycles of equal length, then n divides $r^2n(n-1)/2-r$.*

Proof. Let $a_1, \cdots, a_r$ be r nonunit elements of G, no two of them from the same inverse-cycle. Then a_mJ^h, with $m=1, \cdots, r$ and $h=0, \cdots, n-1$, ranges through all nonunit elements of G. Now let k be any integer, $0<k\leqq r$; then for any fixed k, m, h, there are uniquely determined q and p such that

$$a_qJ^p\cdot a_k = a_mJ^h, \tag{22}$$

except in the cases $k=m$ where h has to be assumed to be nonzero. Let now k, m, h run independently through all possible values. Then, with h ranging through n values and k and m each ranging through r values, but with r equations with $h=0$ excluded, there are r^2n-r distinct equations (22). We sum now the h's of all these equations:

$$\sum h = r^2(0+1+\cdots+n-1)-r\cdot 0 = r^2n(n-1)/2. \tag{23}$$

Using the automorphic-inverse property we can write (22) in another form:

$$a_q\cdot a_kJ^{-p} = a_mJ^{h-p}. \tag{24}$$

Since each Equation (22) yielded a unique Equation (24) and since also the converse is true, we have here again r^2n-r distinct equations. These are all possible equations of the type $a_ib=c$, where b and c are nonunit loop elements, and a_i is defined as above. Hence q ranges through 1, 2, $\cdots$, r, and for each of its values, a_kJ^{-p} runs through all the rn nonunit loop elements except a_qJ^1, because in that case the right hand side would become 1 and could not be expressed as a_mJ^{h-p}. Now we sum (mod n) the $-p$ over all the r^2n-r equations (24) and get

$$\begin{aligned}\sum(-p) &\equiv r(r(0+1+\cdots+n-1)-1)\\ &\equiv r^2(n-1)/2-r \pmod n.\end{aligned} \tag{25}$$

The right hand side of (24) ranges in the r^2n-r distinct equations through the nonunit elements, once for each value of q in the first term of the left hand side, a_q. The only loop element which a_mJ^{h-p} cannot equal for a given q is $a_qJ^0=a_q$ because $a_kJ^{-p}\neq 1$. Now we sum (mod n) the $h-p$ for all the r^2n-r equations (24) and get

$$\sum(h-p) \equiv r(r(0+1+\cdots+n-1)-r\cdot 0)) \pmod n,$$

or $\sum h+\sum(-p)\equiv r^2n(n-1)/2 \pmod n$. Combining this congruence with (23) and (25) we have $r^2n(n-1)/2+r^2n(n-1)/2-r\equiv r^2n(n-1)/2 \pmod n$, $r^2n(n-1)/2-r\equiv 0 \pmod n$. This completes the proof.

For $n=1$ and $n=2$ the requirement of Theorem 8 is always fulfilled. For the more interesting case $n>2$ (because then I.P. loops and groups are excluded) the smallest possible loop orders are 10, with $n=r=3$, and 17, with

$n=r=4$. For these cases the author has constructed multiplication tables; in the first case the constructed loop cannot be C.I., as can be proved. In the second case actually constructed examples show that the loop may be C.I. but is not necessarily C.I.

The condition of Theorem 8 implies the condition $n \mid 2r$, which was mentioned in [1], but the condition of the present theorem is stronger, as can be easily verified for the example $n=4$, $r=6$.

Added in proof. In a more recent paper by Toshiharu Ikuta (Nat. Sci. Rep. Lib. Arts Sci. Fac. Shizuoka Univ. vol. 2 (1957) pp. 1–4) appears a theorem equivalent to Theorem 8: Under the same assumptions, $r \equiv 0 \pmod{n}$ for even r, $2r \equiv 0 \pmod{n}$ for odd r.

3. **Construction of infinite automorphic-inverse loops.** In the following, a method of construction will be described; each of the constructed automorphic-inverse loops satisfies also another identity. The method is an elaboration and generalization of the technique used for the construction of C.I. loops in [1].

Let the infinite multiplicative group $\{J\}$ serve as the multiplicative group of a neofield $(N, +, \cdot)$. Our aim is to construct stepwise the loop $(N, +)$. In addition to the powers of J, including $J^0=1$, N contains only the element 0 with the rules $x \cdot 0 = 0 \cdot x = 0$ and $x+0=0+x=x$, all x in N. We postulate $J^n+J^{n+1}=0$ for all integers n. Thus J has now in $(N, +)$ the same meaning as in 1.11, and the distributive law of $(N, +, \cdot)$ signifies the automorphic-inverse property of $(N, +)$.

Let the function θ be defined by $J^0+J^{k+1}=J^{k\theta}$ for all nonzero integers k. Thus $J^a+J^b=J^{a+(b-a-1)\theta}$ for all integers a and b, $b \neq a+1$; hence knowing $k\theta$ for every nonzero k suffices for complete knowledge of $(N, +)$. In order to assign, step by step, values to $c\theta$ for given integers c, we use a suitable function ϕ with $\phi^n=I$, where $n>1$ is an integer. An easy way of selecting such functions is developing them from functions of the form $r(x+q)^{-1}$ or $px+r$ over some field, where $p=1$ or -1, q and r integers. Two examples will explain the method of construction.

3.1. The function $x\Phi=a-x$ over the real numbers, a being an integral constant, satisfies $\Phi^{2k}=I$, k an arbitrary positive integer. The function can be "translated" into a function in $(N, +, \cdot)$ in various ways, for instance

$$xf = a + xJ, \tag{26}$$

or if $x=J^y$, $a=J^b$, then $J^{y\phi}=J^b+J^{y+1}$ for $y \neq b$. Thus $J^{y\phi}=J^{b+(y-b)\theta}$ and $y\phi=b+(y-b)\theta$. We postulate now $\phi^{2k}=I$ which cannot lead to a contradiction because then also $\Phi^n=I$, in the more special neofield of real numbers, would be contradictory. It can be easily verified that $y\phi^{2k}=b+(y-b)\theta^{2k}$, and if $\phi^{2k}=I$, this becomes

$$y - b = (y - b)\theta^{2k}. \tag{27}$$

Now $\Phi^{2k}=I$ is equivalent to $f^{2k}=I$, and by developing this according to (26) we obtain

$$xJ^{2k}L(aJ^{2k-1})L(aJ^{2k-2})\cdot\cdot\cdot L(aJ)L(a) = x. \tag{28}$$

If we construct a loop according to the rule (27) then the identity (28) will be valid in this loop. The actual construction will be described now for the case $b=3$, $k=2$. We assign the function values of θ stepwise in some specified order as, for instance, 0, 1, -1, 2, -2, $\cdots$; but we omit values leading to coincidences and undefined values as 0θ, $0\theta^{-1}$, $c\theta=c+1$. Also the period $2k=4$ has to be observed. Proceeding in accordance with this rule we obtain $1\theta=-1$, $1\theta^2=(-1)\theta=2$, $1\theta^3=2\theta=-3$, $1\theta^4=(-3)\theta=1$, $(-2)\theta=3$, $3\theta=-4$, $(-4)\theta=4$, $4\theta=-2$, etc.

This example yielded $(N, +)$ as an automorphic-inverse loop with the identity (28) which can be considered as a specialization of the left I.P. identity. If we had chosen some other order in assigning the values of θ we should have obtained another $(N, +)$ with the same properties, but in general these different $(N, +)$'s are not isomorphic to each other.

3.2. As a second example we choose $x\Phi=(1-x)^{-1}$ over the real numbers $x\neq 1$. We have $\Phi^3=I$. A suitable "translation" of the function for $(N, +, \cdot)$ is

$$xf = (1 + xJ)^{-1} \tag{29}$$

or, with $x=J^v$, $J^{v\phi}=(1+J^{v+1})^{-1}=J^{-v\theta}$,

$$y\phi = -y\theta, \quad \text{and} \quad y\phi^3 = y = (-(-y\theta)\theta)\theta. \tag{30}$$

We postulate now $f^3=I$, according to $\Phi^3=I$. Thus we obtain

$$(1 + xJ) + J = ((x + x^2J) + xJ) + (xJ + x^2J^2). \tag{31}$$

Our procedure would yield a loop $(N, +)$ with the identity (31), but since the identity is rather cumbersome, we use an auxiliary condition. The function Φ satisfies evidently the relation $-x\cdot x\Phi\cdot x\Phi^2=1$, and we postulate as an analogous auxiliary condition

$$xJ\cdot xf\cdot xf^2 = 1 \tag{32}$$

which becomes, after substituting (29), $(1+xJ)+J=xJ$. This identity is equivalent to the C.I. property of the automorphic-inverse loop. The identity (31) follows from the C.I. property, thus it is consistent with it. From the identity (32) follows, with $x=J^v$,

$$y + 1 - y\theta = (-y\theta)\theta \tag{33}$$

as auxiliary condition which is consistent with (30). Now, with (30) and (33), the loop can be constructed along the lines indicated in 3.1. This construction of a C.I. loop is described in detail in [1].

3.3. Another example, not worked out here, is $x\Phi = x - 1$ over a field of characteristic k. Obviously $\Phi^k = I$. The neofield "translation" that we choose is $xf = x + J$. This function yields an automorphic-inverse $(N, +)$ with the identity $xR(J)^k = x$.

All the neofields $(N, +, \cdot)$ thus constructed have the same properties that have been proved [6] for the case of 3.2: They are monogenic, their order is countable, their additive loops are simple; and by modifying the order of the steps by which the respective additive loop is constructed, uncountably many nonisomorphic loops $(N, +)$ can be produced [cf. 7].

References

1. R. Artzy, *On loops with a special property*, Proc. Amer. Math. Soc. vol. 6 (1955) pp. 448–453.

2. ———, *A note on the automorphisms of special loops*, Riveon Lematematika vol. 8 (1954) p. 81.

3. ———, *Loops and generally situated* 4*-webs*, Scientific Publications of Technion, Israel Institute of Technology vol. 6, 1954–1955, pp. 5–13.

4. R. H. Bruck, *Contributions to the theory of loops*, Trans. Amer. Math. Soc. vol. 60 (1946) pp. 245–354.

5. ———, *On a theorem of R. Moufang*, Proc. Amer. Math. Soc. vol. 2 (1951) pp. 144–145.

6. ———, *Analogues of the ring of rational integers*, Proc. Amer. Math. Soc. vol. 6 (1955) pp. 50–58.

7. T. Evans, *Some remarks on a paper by R. H. Bruck*, Proc. Amer. Math. Soc. vol. 7 (1956) pp. 211–220.

Israel Institute of Technology,
Haifa, Israel
University of Wisconsin,
Madison, Wis.