On ideals in over-rings

By A. D. SANDS (Dundee)

It is well known that the concept of ideal is not a transitive relation. In this paper we consider cases when the transitive property does hold. We work in the category of associative rings, but do not assume that each ring has an identity element.

We use the notation $A \lhd B$, $A \lhd_l B$, $A \lhd_r B$ to mean that A is an ideal, a left ideal, a right ideal of the ring B, A subring A of the ring B is said to be (left, right) accessible in B if there is a chain of subrings

$$A = A_0 \subset A_1 \subset \ldots \subset A_{n-1} \subset A_n = B$$

such that A_i is a (left, right) ideal of A_{i+1} for $i=0, 1, \ldots, n-1$. We denote by $(1, B)$ the usual extension with identity of the ring B. If $b \in B$ we denote by (b), $(b)_l$, $(b)_r$ the ideal, left ideal, right ideal of B generated by b. The middle annihilator of a ring B is defined by $A_{nn_m}(B) = \{b \in B \mid BbB = 0\}$. Z denotes the ring of integers.

Ring extensions were first considered by EVERETT [2] and later by RÉDEI [6, 7], and by HOCHSCHILD [3] and MACLANE [4], who used a homological treatment. An account of Rédei's work is to be found in his book [8]. More recently PETRICH [5] has recast results of EVERETT and RÉDEI. RÉDEI defines a double homothetism of a ring B to be a pair of mappings (λ, ϱ), where λ is a homomorphism of the right module B_B and ϱ is a homomorphism of the left module ${}_BB$ such that for all $a, b \in B$ we have

(i) $a(\lambda b) = (a\varrho)b$,

(ii) $(\lambda b)\varrho = \lambda(b\varrho)$.

Here we are writing the mapping λ on the left and the mapping ϱ on the right. If one considers only pairs of homomorphisms satisfying (i), called bimultiplications by MACLANE, they form a ring with respect to pointwise addition and composition of mappings as multiplication. However the double homothetisms need not form a subring in this ring. Given a double homothetism (λ, ϱ) the subring of the ring of bimultiplications generated by (λ, ϱ) consists of all polynomials in (λ, ϱ) with integer coefficients and zero constant term. It is easy to verify that each of these is a double homothetism. If $B \lhd C$ then for each $c \in C$ the pair of mappings (λ_c, ϱ_c) given by $\lambda_c(b) = cb$, $(b)\varrho_c = bc$, for each $b \in B$, is a double homothetism of B. Thus if $A \lhd B$ and $\lambda A \subset A$, $A\varrho \subset A$ for all double homothetisms (λ, ϱ) of B then $A \lhd C$ for all over-rings C of B such that $B \lhd C$. Rédei's result is that the converse also holds. If H is any *ring* of double homothetisms of B then the additive abelian group $B \oplus H$ may be made into

L, any two elements a, b of L can be used to define another operation on L as follows: $x^*y=XY$ where X, Y are the unique solutions of the equations $Xa=x$ and $bY=y$ in L. $(L, ^*)$ is a loop and is called a principal isotope of L. The representation of $(L, ^*)$ will be $\{R(a)^{-1}R(u);\ u \text{ in } L\}$. An autotopism of L is a triple (U, V, W) of permutations of L such that for all x, y in L, $(xU)(yV)=(xy)W$.

General results

Proposition 1. *The following are equivalent on any loop L:*

(i) *L is a right central loop*

(ii) *L is right alternative and for all x in L, x^2 belongs to the right nucleus of L.*

(iii) *$(I, R(x)^2, R(x)^2)$ is an autotopism of L (Here I denotes the identity permutation on L)*

(iv) *If A, B belong to $R(L)$ then AB^2 also belongs to $R(L)$.*

(v) *$L(x)R(y)^2=R(y)^2L(x)$ for all x, y in L (Here $L(x)$ denotes left multiplication by x).*

PROOF. *(i)* implies *(ii)* has been noted by FENYVES [4]. To prove the converse, note that $(zy)x^2=z(yx^2)$ for all z, y, x in L since x^2 is in the right nuleus. By right alternativity, the left side of this equation is $((zy)x)x$ and the right side is $z((yx)x)$ and the right central identity follows.

(i) implies *(iv)* because, if $A=R(y)$ and $B=R(x)$, then by the right central identity $zAB^2=zC$ where $C=R(yx\cdot x)$. Thus AB^2 is in $R(L)$. Conversely, if AB^2 is in $R(L)$ then it is equal to some $R(t)$. So, $t=eR(t)=eAB^2=((ey)x)x=(yx)x$. Now for any z in L, $((zy)x)x=zAB^2=zR(t)=zt=z((yx)x)$ so that L is a right central loop.

(iii) and *(v)* are just restatements of the right central identity in appropriate symbols.

Corollarry 2. *Any loop of exponent 2 (i.e. each x satisfies $x^2=e$) which is either right alternative or has the right inverse property is a right central loop. Hence if the representation of a loop consists of permutations of order at most 2 then the loop will be a right central loop.*

PROOF. Follows from (i) and (iv) above.

Corollary 3. *A Bol loop (resp. a right central loop) will be a right central loop (resp. a Bol loop) if and only if, for all x in the loop, $(R(x), R(x)L(x)^{-1}, R(x))$ is an autotopism.*

PROOF. The autotopisms of any loop form a group. Further, a loop L is a Bol loop if and only if $(R(x)^{-1}, L(x)R(x), R(x))$ is an autotopism for all x in L. (Theorem 2.3, ROBINSON [7]). Hence the corollary follows from *(iii)* of Proposition 1 and the equation $(R(x)^{-1}, L(x)R(x), R(x))=(R(x)^{-1}, L(x)R(x)^{-1}, R(x)^{-1})\cdot\cdot(I, R(x)^2, R(x)^2)$.

Corollary 4. *The following are equivalent on any loop L:*

(i) Any loop isotopic to L is a right central loop.

(ii) For all A, B, C in $R(L)$, $A(B^{-1}C)^2$ also is in $R(L)$.

Any loop satisfying the above conditions is a Bol loop.

PROOF. *(i)* implies (ii): The set $\{B^{-1}D;\ D \text{ in } R(L)\}$ defines the representation o a principal isotope L' of L, for any B in $R(L)$. If L' is a right central loop, then $(B^{-1}A)(B^{-1}C)^2$ is in $R(L')$ for all A, C in $R(L)$, by (iv) of Proposition 1. Let $(B^{-1}A)(B^{-1}C)^2 = B^{-1}D$. Then $A(B^{-1}C)^2 = D$ belongs to $R(L)$.

(ii) implies (i): Let L' be a principal isotope of L. Then $R(L') = \{B^{-1}D;\ D \text{ in } R(L)\}$ for some fixed B in $R(L)$. Let $B^{-1}A$, $B^{-1}C$ be two elements of $R(L')$ with A, C in $R(L)$. By (ii), $D = A(B^{-1}C)^2$ belongs to $R(L)$. Therefore $B^{-1}D = (B^{-1}A) \cdot \cdot (B^{-1}C)^2$ belongs to $R(L')$. Thus L' is right central.

If L satisfies *(ii)*, then taking $A = B$, we have $CB^{-1}C$ belongs to $R(L)$ for all C, B in $R(L)$ which is equivalent to L being Bol (Theorem 1, BURN (3), I).

Lemma 5. *The following properties are true in any right central loop L.*

(i) For any element, the right inverse equals the left inverse.

(ii) If s is the square of some element of L and x is any element of L, then $(xs)^{-1} = s^{-1}x^{-1}$.

(iii) The order of any element is a divisor of the order of L.

PROOF. *(i)* Let y be the right inverse and z be the left inverse for the element x. Then $yy = ey \cdot y = (zx \cdot y)y = z(xy \cdot y) = zy$ and so $y = z$.

(ii) Since s belongs to the right nucleus, $(s^{-1}x^{-1})(xs) = ((s^{-1}x^{-1})x)s = = (s^{-1}(x^{-1}x))s = s^{-1}s = e$.

(iii) As shown in Fenyves (4), Theorem 3, $(xy^m)y^n = xy^{m+n}$ for all x, y in L and for all integers m, n. Using this, it is easy to check that the left cosets of any subgroup generated by a single element form a partition of L. Since each member of this partition will contain exactly the same number of elements as the order of the generator of the subgroup, the result follows.

Proposition 6. *Any right central loop of odd order is a group*

PROOF. If $2n+1$ is the order of the loop, then by *(iii)* of the above lemma, $x^{2n+1} = e$ for all x. Hence $(x^{n+1})^2 = x$ for all x. Thus, by (ii) of Proposition 1, every x belongs to the right nucleus and hence the loop is associative.

Construction

We now establish the following by suitable constructions:

(A) For every even integer $2m$ where $m > 3$ there exists a non-Bol right central loop of order $2m$.

(B) For every integer of the form $4k$ where: $k > 2$ there exists a non-Moufang loop of order $4k$ which is both Bol and right central.

(C) For every integer of the form $2n^2$ where $n > 2$ and $n \neq 4, 8$ there exists a non-Moufang Bol loop of order $2n^2$ which is not right central.

PROOF. (A) Let $2m = n+1$ and $n = 2k+1$ where $k > 0$. Consider the set $X = \{e, 0, 1, 2, \ldots, n-1\}$ where e is an arbitrary symbol. For $r = 1$ through n, let P_r be the permutation which is the product of the 2-cycles $(e, r), (r+1, r-1), (r+2, r-2), \ldots, (r+k, r-k)$ where all the integers are reduced modulo n. Let P_0 be the idenity permutation on X. Then the 2m permutations P_i, $i = 0, \ldots, n$ form a right regular representation of a loop $(X, .)$ of order $2m$ on the set X. This can be established by verifying the conditions of Theorem 1 of BURN (3, I) (It would be helpful to consider $0, 1, \dots, n-1$ as points on a circle in that order and the 2-cycles in P_i as chords joining points symmetrically on opposite sides of the point i) The loop $(X, .)$ is right central since all the permutations P_i are of order at most 2. But it is not a Bol loop because $3P_2P_3P_2=2k=3P_1$ and $2P_2P_3P_2=1\neq 2P_1$ and hence $P_2P_3P_2$ cannot be equal to any P_i voilating the condition of Theorem 3 of Burn (3, I).

(B) We use a construction given by Robinson (8). Let G be a group generated by two elements a, b such that $a^2=b^2=1$ and $ab=ba$. Let H be a cyclic group of order k $(k\geqq 3)$. Define a map f: $G\to \mathrm{Aut}(H)$ by $f(1)=u$, $f(a)=f(b)=f(ab)=v$ where u is the identity automorphism and v is the automorphism $x\to x^{-1}$. Now define a multiplication on the set product $B=GxH$ by $(y, b)(x, a)=(yx, (f(x))(b)a)$ for all y, x in G, b, a in H. Then B is a non-Moufang Bol loop of order $4k$. It is obvious that the square of each element of B has the identity as its first coordinate. Since any such element lies in the right nucleus of B it follows that B is a right central loop.

(C) This construction is similar to the one in (B). Let G be the dihedral group of order $2n$ with genrators a, b where $a^n=e$, $b^2=e$, $ab=ba^{-1}$. Define f: $G\to \mathrm{Aut}(G)$ by $f(x)=$the inner automorphism induced by x^{-1}. Then the set $G\times G$ with the product $(y, b)(x, a)=(yx, f((x))(b)a)$ is a non-associative Bol loop and the subset $L=\{(a^kb^m, b^ma^l),\ 0\leqq k, l\leqq n-1,\ m=0, l\}$ is a non-Moufang subloop which is a Bol loop of order $2n^2$. Taking the elements $x=(b, b)$, $y=(a, e)$ in L, we get $(xx)y^2\neq \neq x(xy^2)$ if n is not a divisor of 8. Thus y^2 does not belong to the right nucleus of L and so L is not a right central loop.

References

[1] G. BOL, Gewebe und gruppen, *Math. Ann.* **114** (1937), 414—431.
[2] R. H. BRUCK, A Survey of Binary Systems, *Springer Verlag*, 1958.
[3] R. P. BURN, Finite Bol loops, I, II, *Math. Proc. Cambridge Phil. Soc.*, **84** (1978), 377—385, **88** (1981), 445—455.
[4] F. FENYVES, Extra loops II, *Publ. Math. Debrecen* **16** (1969), 187—192.
[5] R. MOUFANG, Zur structur von Alternativekorpen, *Math. Ann.*, **110** (1935), 416—430.
[6] H. NIEDERREITER and K. H. ROBINSON, Bol loops of order pq, *Math. Proc. Cambridge Phil. Soc.* **89** (1981), 241—256.
[7] D. A. ROBINSON, Bol loops, *Trans. Amer. Math. Soc.* **123** (1966), 341—354.
[8] K. H. ROBINSON, A note on Bol loops of order 2^nk, *Aequationes Mathematicae* **22** (1981), 302—306.

(RAMAMURTHI) DEPARTMENT OF MATHEMATICS,
UNIVERSITY OF NORTH FLORIDA,
JACKSONVILLE, FL 32216, USA
(SOLARIN) DEPARTMENT OF MATHEMATICS,
UNIVERSITY OF IFE, ILE-IFE, NIGERIA.

(Received April 3, 1986.)