

## PAIRS OF INVERSE MODULES IN A SKEWFIELD

F. W. LEVI

Let  $\Sigma$  be a skewfield. If  $J$  and  $J'$  are submodules of  $\Sigma$  such that the nonzero elements of  $J$  are the inverse elements of those of  $J'$ , then  $J$  and  $J'$  form a "pair of inverse modules." A module admitting an inverse module will be called a  $J$ -module and a selfinverse module containing 1 will be called an  $S$ -module. In an earlier paper<sup>1</sup> the author has shown that if  $\Sigma$  is a (commutative) field of characteristic not equal to 2, then every  $S$ -module is a subfield of  $\Sigma$ . Only in fields of characteristic 2, nontrivial  $S$ -modules can be found. A corresponding distinction of that characteristic does not hold for skewfields. Even the skewfield of the quaternions contains nontrivial  $S$ -modules, for examples the module generated by 1,  $j$ ,  $k$ . In the present paper some properties of  $S$ -modules and  $J$ -modules will be discussed. For example it will be proved that when an  $S$ -module contains the elements  $a$ ,  $b$  and  $ab$ , it contains all the elements of the skewfield which is generated by  $a$  and  $b$ . By a similar method it will be shown that finite  $S$ -modules are necessarily Galois-fields.

### 1. Necessary and sufficient conditions for $J$ -modules.

**THEOREM 1.** *A submodule  $J$  of  $\Sigma$  is a  $J$ -module if and only if  $a \in J$  and  $b \neq 0 \in J$  imply  $ab^{-1}a \in J$ .*

**PROOF.** Let  $J$  be a  $J$ -module. Without loss of generality suppose that  $a \neq 0$ ,  $b - a = c \neq 0$ . Then  $k = a^{-1} + c^{-1} \in J'$  since  $J'$  is closed under addition and subtraction. As  $k = a^{-1}(c + a)c^{-1}$ ,  $k^{-1} = cb^{-1}a$ ; hence  $a - k^{-1} = ab^{-1}a$  is contained in  $J$ . Let now  $J$  be a module satisfying the condition mentioned above. To prove that  $J$  is a  $J$ -module, we shall show that when  $a$  and  $c$  are nonzero elements in  $J$ , but otherwise arbitrary, then  $a^{-1} + c^{-1}$  is either 0 or the inverse of an element of  $J$ . The first alternative holds when  $b = a + c = 0$ ; if however  $b \neq 0$ , then  $a^{-1} + c^{-1} = (a - ab^{-1}a)^{-1}$  is the inverse of an element of  $J$ . Hence the theorem.

**COROLLARY 1.** *The meet of any (finite or infinite) set of  $J$ -modules in  $\Sigma$  is a  $J$ -module in  $\Sigma$ .*

This corollary shows that the  $J$ -modules in  $\Sigma$  form a lattice with the set-inclusion as the defining order-relation.  $J_1 \wedge J_2$  denotes the ordi-

---

Received by the editors March 4, 1947.

<sup>1</sup> *Pairs of inverse moduls*, J. Indian Math. Soc. N.S. vol. 3 (1936) pp. 295-306.

nary meet, whereas  $J_1 \vee J_2$  is the meet of all the  $J$ -modules in  $\Sigma$  which contain  $J_1$  and  $J_2$ . This lattice is in general not a sublattice of the lattice of all the submodules of  $\Sigma$ .

**COROLLARY 2.** *If  $a$  and  $b$  are elements of  $\Sigma$  and  $J$  is a  $J$ -module in  $\Sigma$ , then  $aJb$  is also a  $J$ -module in  $\Sigma$ .*

**COROLLARY 3.** *If the  $J$ -module  $J$  contains 1, then  $J$  is an  $S$ -module.*

**PROOF.** From  $1 \cdot b^{-1} \cdot 1 \in J$ , follows  $J' \subseteq J$ . As  $1^{-1} = 1 \in J'$ , the inverse inequality holds. Hence  $J = J'$  is selfinverse and contains 1.

**COROLLARY 4.** *If  $a' \in J'$ , then  $a'J = S$  is an  $S$ -module, or the zero-module.*

Therefore every  $J$ -module which contains nonzero elements can be denoted by  $J = aS$ , where  $a \neq 0$  is an otherwise arbitrary element of  $J$ . The  $S$ -module  $S$  depends on the selection of  $a$ . For the following proofs, it is important to remember that when  $a$  and  $b$  belong to an  $S$ -module  $S$ , then

$$(1) \quad a + b, \quad a - b, \quad aba, \quad \text{and, for } a \neq 0, \quad a^{-1}$$

also belong to  $S$ .

**COROLLARY 5.** *If  $a \neq 0$  and  $a \in J$ , then  $aJ'a = J$ .*

**PROOF.** From Theorem 1 it follows that  $aJ'a \subseteq J$  and  $a^{-1}Ja^{-1} \subseteq J'$ . The second formula furnishes  $J \subseteq aJ'a$ ; hence the corollary.

In  $S$ -modules (and other selfinverse modules) every element  $a \neq 0$  of  $S$  generates a module-automorphism  $S \rightarrow aSa$ .

**2. Skewfields in  $S$ -modules.** Obviously the primefield of  $\Sigma$  is contained in every  $S$ -module of  $\Sigma$ . We shall investigate now the conditions for  $S$  to contain the skewfield

$$(2) \quad F(a, b)$$

which is generated in  $\Sigma$  by the elements  $a$  and  $b$  (that is, the meet of all the sub-skewfields containing  $a$  and  $b$ ). That  $S$  may contain  $a$  and  $b$  but not  $F(a, b)$  appears from the example mentioned above, where  $\Sigma$  is the skewfield of the quaternions and  $S$  is the module generated by  $1, j, k$ .

**LEMMA 1.** *If an  $S$ -module  $S$  contains  $a \neq 0$ , it contains  $a^m$  (for  $m = 0, \pm 1, \pm 2, \dots$ ).*

**PROOF.** It suffices to prove the lemma for positive exponents.  $S$

contains  $a$  and  $a1a = a^2$  and with  $a^m$ , also  $aa^m a = a^{m+2}$ . Hence the lemma follows by mathematical induction.

**THEOREM 2.** *If an  $S$ -module  $S$  contains  $a, b$  and  $ab$  it contains all the elements of  $F(a, b)$ .*

**PROOF.** Without loss of generality, suppose that  $a, b \neq 0$ .  $S$  contains  $a^{-1} \cdot ab \cdot a^{-1} = ba^{-1}$ , hence  $ab^{-1}$  and  $b \cdot ab^{-1} \cdot b = ba$ . The suppositions are therefore symmetric for left and right and for  $a$  and  $b$ . Herefrom it follows that  $a^\epsilon b^\delta$  and  $b^\delta a^\epsilon$  belong to  $S$  for  $\epsilon, \delta = \pm 1$ . If  $a^r b^s \in S$  then  $a^{\pm r} b^{\pm s} \in S$  and  $b^{\pm s} a^{\pm r} \in S$ . To show that all the terms  $a^r b^s$  belong to  $S$ , we may therefore restrict ourselves to positive values of  $r$  and  $s$ . Suppose  $ab^m \in S$  for  $0 \leq m \leq n$ . This formula holds for  $n = 1$ . Moreover  $S$  contains  $b \cdot ab^{n-1} \cdot b = bab^n$ . As  $S$  is supposed to contain  $b$  and  $ab^m$ , it must also contain  $ab^{n+1}$ . Hence it follows by mathematical induction that  $ab^m \in S$  for every positive  $m$  and therefore  $b^m a \in S$ . We can now substitute  $b^m$  for  $a$  and  $a$  for  $b$  and obtain by the same conclusion that  $b^m a^r \in S$  for every positive  $r$  and finally we see that for all the integral values of  $r$  and  $s$ , the elements  $a^r b^s$  and  $b^s a^r$  belong to  $S$ . Let now  $R$  be the ring generated by  $a, b, a^{-1}, b^{-1}$ . The elements of  $R$  can all be represented as sums of terms

$$(3) \quad \pm a^{r_1} b^{s_1} \cdots a^{r_n} b^{s_n},$$

where the exponents take the values  $0, \pm 1, \pm 2, \dots$ . To prove that  $R \subseteq S$ , it suffices to show that all the elements (3) belong to  $S$ . The statement has been proved for  $n = 1$ . Now  $(b^{-u} a^{-v} \cdot a^{r_1} b^{s_1} \cdots a^{r_n} b^{s_n} \cdot b^{-u} a^{-v})^{-1} = a^v b^{u-s_n} a^{-r_n} \cdots b^{-s_1} a^{v-r_1} b^u$ . When  $u, v, r_1, \dots, r_n, s_1, \dots, s_n$  run independently over all the integral numbers, then the same holds for the  $2n + 2$  exponents on the right-hand side. Thus one obtains by mathematical induction that  $R$  is contained in  $S$ . For the last steps of the proof one needs the following lemmas:

**LEMMA 2.** *If an  $S$ -module  $S$  contains a ring  $R$ , then  $S$  contains also a ring in which the elements of  $R$  and their inverse elements occur.*

**PROOF OF LEMMA 2.** The ring generated by the elements  $\alpha_i, \alpha_k, \dots$  of  $R$  and their inverse elements consists of sums of terms of the type

$$(4) \quad \alpha_1 \alpha_2^{-1} \cdots \alpha_{2n-1} \alpha_{2n}^{-1};$$

the element 1 can be used as an  $\alpha$  as well as an  $\alpha^{-1}$ . To show that this ring is contained in  $S$ , it suffices to show that every element of type (4) belongs to  $S$ . As  $\alpha_i, \alpha_k$  and  $\alpha_i \alpha_k$  belong to  $S$ , the same holds for  $\alpha_i \alpha_k^{-1}$ ; hence the statement is true for  $n = 1$ . To prove it for an

arbitrary  $n$  by mathematical induction, we observe that every product of  $\alpha$ 's is an  $\alpha$  and that the corresponding holds for the inverse elements. Thus

$$(\alpha_1\alpha_3\cdot\alpha_4^{-1})(\alpha_4\cdot\alpha_3^{-1}\alpha_2^{-1}\alpha_1^{-1})(\alpha_1\alpha_3\cdot\alpha_4^{-1}) = \alpha_1\alpha_2^{-1}\alpha_3\alpha_4^{-1} \in S.$$

Moreover if the statement holds for any particular  $n > 1$ , it follows that

$$\begin{aligned} &(\alpha_1\alpha_{2n+1}\alpha_{2n+2}^{-1})(\alpha_{2n+2}\alpha_{2n+1}\alpha_2^{-1}\cdot\alpha_3\alpha_4^{-1}\cdot\cdot\cdot\alpha_{2n-1}\alpha_{2n}\alpha_1^{-1})(\alpha_1\alpha_{2n+1}\alpha_{2n+2}^{-1}) \\ &= \alpha_1\alpha_2^{-1}\cdot\alpha_3\alpha_4^{-1}\cdot\cdot\cdot\alpha_{2n-1}\alpha_{2n}^{-1}\alpha_{2n+1}\alpha_{2n+2}^{-1} \in S. \end{aligned}$$

Hence we have Lemma 2.

**LEMMA 3.** *If an  $S$ -module  $S$  contains a ring  $R$ , it contains also a skewfield  $F \supseteq R$ .*

**PROOF OF LEMMA 3.** From Lemma 2 follows the existence of a ring  $R'$  such that  $R \subseteq R' \subseteq S$  and  $R'$  contains also the elements which are inverse to those of  $R$ . If  $R'$  contains the inverse elements of all its elements, then it is a skewfield; at any rate it is a subring of a subring  $R''$  of  $S$  which contains those inverse elements. By continuing this procedure, one obtains an ascending chain of subrings  $R, R', R'', \dots$  in which each ring contains the preceding rings and their inverse elements. The join of these rings is a skewfield  $F$ . Hence we have the lemma.

As, under the suppositions of Theorem 2,  $S$  has a subring  $R$  which contains  $a$  and  $b$ , the module  $S$  has also a sub-skewfield  $F$  which contains  $R$  and therefore  $a$  and  $b$ . Hence  $S \supseteq F \supseteq F(a, b)$ .

**COROLLARY.** *When a  $J$ -module  $J$  contains  $a, b, c$  and  $d$ , where  $ab^{-1}cd^{-1} = 1$ , then  $J$  contains  $dF(d^{-1}c, d^{-1}a)$ .*

**PROOF.**  $d^{-1}J$  is an  $S$ -module which contains  $d^{-1}c, d^{-1}a$  and  $d^{-1}b = d^{-1}cd^{-1}a$ .

**3. Finite  $S$ - and  $J$ -modules.** Let  $0, a_1, a_2 \dots$  be the elements of an  $S$ -module  $S$  in  $\Sigma$ .

Every "word" of the type

$$(5) \quad a_1a_2 \dots a_n$$

belongs to the ring  $A$  generated by  $S$ . As every  $-a_i$  is also an  $a$ , each element of  $A$  can be represented as a sum of words (5). Furthermore the sum of the two equal terms can be contracted into a single one, say  $2a_1 \cdot a_2 \dots a_n$ , since  $2a_1$  is also an element  $a$ . Thus we can

suppose that the terms in a sum which represent an element of  $A$  are all different. In general such a term affords different representations as a word (5). For the shortest representation, the following lemma holds.

**LEMMA 4.** *In the shortest representation (5) of a product of nonzero elements of  $S$  all the letters  $a_i$  are different.*

**PROOF.** Suppose that in (5) the same letter  $a$  occurs several times, say  $aa_1 \cdots a_m a$  is a portion of a product of type (5). We replace every  $a_{2k}$  by  $aa^{-1}a_{2k}a^{-1}a$ . Now  $aa_{2k-1}a = a'_{2k-1}$  and  $a^{-1}a_{2k}a^{-1} = a'_{2k}$  are also elements of  $S$ . Hence the product under consideration is reduced to  $a'_1 \cdots a'_m$  when  $m$  is odd and to  $a'_1 \cdots a'_m a^2$  when  $m$  is even. As  $a^2 \in S$ , the length of the product has been reduced by the operation. Thus in a shortest representation, no repetition of elements can occur.

It may be mentioned that in a  $J$ -module which does not contain 1, no square of any element  $a \neq 0$  of  $J$  is contained, since  $a^2 \in S$  implies  $a \cdot a^{-2} \cdot a = 1 \in S$ . The lemma therefore does not hold for  $J$ -modules. However one can show by the same method that when the module formed by the  $a$ 's is selfinverse, in the shortest representation (5) no letter occurs more than twice.

**THEOREM 3.** *Every finite  $S$ -module  $S$  is a Galois field.*

**PROOF.** If  $n$  is the number of elements of  $S$ , then it follows from Lemma 4 that there exist only  $m \leq n^n$  different products of such elements. The ring  $R$  generated by  $S$  consists of sum of different products and therefore  $R$  has not more than  $2^m$  elements. In a finite ring, every element  $a$  generates a finite multiplicative cyclic group; hence  $R$  contains  $a^{-1}$ .  $R$  is therefore a skewfield and as  $R$  is finite, it is a Galois field.<sup>2</sup>  $S$  is therefore an  $S$ -module in a Galois field.  $S$ -modules in (commutative) fields are known<sup>3</sup> to be subfields, except in the case of characteristic 2. It remains to prove the theorem for the case when  $S$  is an  $S$ -module in  $GF_{2^r}$ . It has been proved<sup>4</sup> that the elements of  $GF_{2^r}$  which multiplied with the elements of  $S$  give elements of  $S$  form a field  $M(S)$  and that  $a \in S$  implies  $a^2 \in M(S)$ . As  $1 \in S$ , we have  $M(S) \subseteq S$ . In a Galois field of order  $2^r$ ,  $a = a^{2^r}$ . Therefore  $a^2 \in M(S)$  implies  $a \in M(S)$ . Hence  $S = M(S)$ . This finishes the proof.

<sup>2</sup> J. H. Maclagan Wedderburn, Trans. Amer. Math. Soc. vol. 6 (1905), p. 349; see also E. Witt, Abh. Hamburgischen Univ. Math. Sem. vol. 8 (1931) p. 413.

<sup>3</sup> Loc. cit. footnote 1, Proposition 4.

<sup>4</sup> Loc. cit. footnote 1, Proposition 2.

**COROLLARY.** *Every finite  $J$ -module is of the form  $aG$  where  $G$  is a Galois field.*

If in particular the finite  $J$ -module is self-inverse, then  $a^2 \in G$ . In the case of Galois fields of characteristic 2, this relation implies  $a \in G$  and therefore  $J = G$ .

**4. Additional remarks.** Let  $S$  be an  $S$ -module in  $\Sigma$  and  $a \in S$ . By  $\mu(a)$  denote the set of those elements  $x \in S$  for which  $ax \in S$ . From Theorem 2 it follows that  $ax^{-1} \in S$ ; moreover  $\mu(a)$  is a module containing 1. Hence  $\mu(a)$  is an  $S$ -module. In the same way, one proves that  $\mu(a) = \mu(a^{-1})$  and that  $\mu(a)$  is also the set of the elements  $x \in S$  for which  $xa \in S$  holds. The meet of all the modules  $\mu(a)$  is a skewfield  $M(S)$ . Two modules  $aM(S)$  and  $bM(S)$  are either identical or they have only the element 0 in common; these modules are  $J$ -modules. Let  $c \in M(S)$  and  $c \neq 0$ , then  $\mu(a) = \mu(ac)$ . Furthermore denote the modules  $xM(S)$  by  $M_1, M_2, \dots$ . For every particular  $c \neq 0$  of  $M(S)$  the mapping  $M_i \rightarrow cM_i$  generates a permutation of the modules  $M_i$  which are subdivided into systems of transitivity.  $M(S)$  forms a system of transitivity by itself. If  $M_1$  and  $M_2$  belong to the same system of transitivity, then  $M_1 = cM_2$ , where  $c \neq 0$ ,  $c \in M(S)$ . As  $M(S) = M(S)c^{-1}$ ,  $M_1 = cM_2c^{-1}$ . Thus the modules belonging to the same system of transitivity are conjugate, the transforming element belonging to  $M(S)$ , and conversely. To every  $M_i$  there corresponds a subskewfield of  $M(S)$  consisting of these elements  $y$  for which  $yM_i = M_i$  or  $yM_i = 0$ . The meet of all these skewfields is a skewfield which contains the prime field of  $\Sigma$ .

CALCUTTA, INDIA