On the general theory of \((m, n)\) rings

J. J. Leeson and A. T. Butson

Abstract. In this paper, the lattice of congruences of an \((m, n)\) ring is determined, a generalization of the Wedderburn theorem for finite division rings is considered, all \((2, n)\) fields, \((2, n)\) rings of prime order, and all \((3, n)\) rings of prime order are determined. A special class of \((2, n)\) fields, called super-simple \((2, n)\) fields, is characterized.

1. Introduction

The study of generalizations of familiar algebraic systems has provided the subject matter for several recent publications, (1), (2), (4), (5), (6), and (8). Dornte, (3), considered a generalized group in 1928. He studied systems with one \(m\)-ary operation subject to associativity laws and to the existence of solutions to equations. Post, (7), called these algebras polyadic groups and thoroughly examined their structure in 1940. In a significant result, referred to herein as the Post Coset Theorem, he showed that an \(m\)-group is a coset of an invariant subgroup, called the associated group, in an ordinary 2-group, called the covering group, and that the corresponding factor group is cyclic of order \(m - 1\). The \(m\)-ary operation in the \(m\)-group is the operation of the cover restricted to products involving admissible numbers of terms from the coset. A product is admissible if the number of terms involved is congruent to \(1\) mod \((m - 1)\). This result is generalized to ring-like algebras in section 4. These algebras, called \((m, n)\) rings, were first examined by Crombez and Timm, (1) and (2), in 1972. Some basic structure theory was established, and a familiar result (embedding an integral domain in a field) was generalized.

The authors would like to thank the referee for a very thorough reading of the original manuscript. The report resulted in a significant improvement in exposition.

Presented by J. D. Monk. Received March 22, 1977. Accepted for publication in final form November 7, 1978.
2. Notation and preliminary results

The theory of polyadic groups and semigroups plays a large role in the investigation of \((m, n)\) rings. Some definitions and results concerning these algebras are included in this section. Details may be found in the papers listed in the bibliography.

**DEFINITION 2.1** An \(m\)-semigroup is an algebraic system \((G, \cdot)\) with one \(m\)-ary operation \(\cdot: G^m \to G\) so that for any set of elements \(g_1, \ldots, g_{2m-1} \in G\) it is true that

\[
((g_1 g_2 \cdots g_m) g_{m+1} \cdots g_{2m-1}) = (g_1 (g_2 \cdots g_{m+1}) g_{m+2} \cdots g_{2m-1}) = \cdots = (g_1 \cdots g_{m-1} (g_m \cdots g_{2m-1})).
\]

An \(m\)-group is an \(m\)-semigroup in which the equations \((g_1 \cdots g_i g_{i+1} \cdots g_m) = g\) each have a unique solution in \(G\) for arbitrary \(g_1, \ldots, g_{m-1}, g \in G\) and for each \(i \in \{0, 1, \ldots, m-1\}\). Further, an \(m\)-semigroup \((m\text{-group})\) is abelian or commutative if the operation is invariant under each permutation of the elements involved.

It is immediate that an ordinary group is a 2-group. It will be assumed throughout this paper that \(m > 1\). Because of the associative laws, parentheses grouping admissible numbers of factors can be omitted with no loss of generality; for instance, the word \(ab\cdots de\) has a unique interpretation in a 3-semigroup. Also, the convention of using \(b^i\) to denote \(i\) copies of \(b\) will be adopted. It is noted that \(b^i\) is meaningless by itself unless \(i\) is congruent to 1 mod \(m-1\). It becomes meaningful, however, as part of an admissible word. It can be referred to as a pre-multiplier and/or as a post-multiplier, as long as the resulting "product" is admissible. Integral coefficients will be used analogously when the operation is expressed additively.

In an \(m\)-group \(G\), the unique solution \(\overline{5}\) to the equation \(b^m y = b\) is called the **quererelement** of \(b\). It has the property that \(b^i b = b^{m-i-1}\) for each \(i = 0, 1, \ldots, m-1\) \((b^0\) acts like a formal identity). When \(m = 2\), \(\overline{5}\) is the identity element of the group for each element \(b\). When \(m > 2\), however, there need not be any relation between \(\overline{5}\) and \(\overline{c}\). Post, (7), has shown that if the \((m-1)-ad\)
\(g_1, \ldots, g_{m-1}\) has the property \(g_1 g_2 \cdots g_{m-1} g = g\) for some \(g \in G\), then it has this property for each \(g \in G\). In this case, \(g_1 g_2 \cdots g_{m-1}\) is called an identity for \(G\). Identities are not unique when \(m > 2\); \(b^i b = b^{m-i-2}\) is an identity for each \(b \in G\), and for each \(i = 0, 1, \ldots, m-2\). An element \(b\) is called an idempotent if \(b^m = b\).

The following result was established by E. L. Post. See (7) for details.