ON A CERTAIN CLASSIFICATION OF RINGS AND SEMIGROUPS

DOV TAMARI

In his paper *Linear equations in non-commutative fields* (Ann. of Math. vol. 32 (1931) pp. 463–477) Professor Oystein Ore defines regularity and irregularity of rings and an "order of irregularity" in such a way that regularity becomes irregularity of order 1. Herewith the following problem is proposed: Do irregular rings of order $n>1$ really exist? If so of what type are they? In this note these questions will be answered. A classification on this line yields nine different types, for which explicit examples are given. This classification turns out to be essentially one of semigroups. For the so-called "ringlike domains," that is, domains having one distributive law only, the position is otherwise and will be treated in detail elsewhere.

The first section of this paper contains the general considerations, the second one the examples.

1. **General considerations.** According to Ore we call a ring without divisors of zero $\mathfrak{R}$ *left-regular* if any two elements a, $b\in\mathfrak{R}$ have a nontrivial[1] common left multiple (C.L.M.), that is, there exists at least one pair of elements x, $y\in\mathfrak{R}$, not both 0, such that $xa=yb$ $=$C.L.M.(a, b). Otherwise we call $\mathfrak{R}$ *left-irregular*. In the same way *right-regularity and right-irregularity* are defined. Another approach to this problem is suggested by the concepts of linear dependence and independence. For the sake of generality we do not exclude rings with nontrivial[2] divisors of zero and define:

If $a_1b_1+\cdots+a_nb_n=\sum a_ib_i=0$, a_i, $b_i\in\mathfrak{R}$, where at least one $b_i\neq 0$, we say that the n elements a_i are *linearly right dependent* (*lin. r. dep.*), and if at least one $a_i\neq 0$, that the n elements b_i are *linearly left dependent* (*lin. l. dep.*). But if for a given set $a_1, \cdots, a_n\in\mathfrak{R}$ it follows from the equation $a_1x_1+\cdots+a_nx_n=\sum a_ix_i$ $=0$ $(x_i\in\mathfrak{R})$ that all $x_i=0$, we say that the set $a_1, \cdots, a_n$ is *linearly right independent* (*lin. r. ind.*). Similarly *linear left independence* (*lin. l. ind.*) is defined.

Obviously a set containing a left (right) divisor of zero is lin. r. (l.) dep.; a set containing a subset, lin. dep. on one side, is itself lin. dep. on the same side. Any subset of a lin. ind. set is therefore also lin.

Received by the editors February 27, 1947.

[1] There exist always the trivial common "one-sided" multiples $0\cdot a=0\cdot b$ and $a\cdot 0=b\cdot 0$ and the "mixed" multiple $xa=by$ with $x=b$, $y=a$.

[2] 0 shall be called a trivial divisor of zero.

indep. on the same side as the set. A set containing equal elements is lin. dep. on both sides. Therefore a lin. r. (l.) ind. set contains only unequal elements, which are not l. (r.) divisors of zero.[3]

If we can find at least one set of n elements $a_1, \cdots, a_n \in \mathfrak{R}$, which is lin. r. indep., and if any set of $(n+1)$ elements of $\mathfrak{R}$ is lin. r. dep., we say, according to Ore, that $\mathfrak{R}$ is of *right order* (*of "irregularity"*) n. Similarly we define the *left order* of $\mathfrak{R}$. But if for any positive integer n there exists in $\mathfrak{R}$ a set of n lin. l. (r.) ind. elements, we say, $\mathfrak{R}$ is of *infinite left* (*right*) *order* and write n_l resp. $n_r = \infty$. We may therefore classify the rings into types (n_l, n_r), where n_l denotes the left, n_r the right order of the ring. Thus for example a ring of type (1, 1) without divisors of zero is regular on both sides in the sense of Ore. Irregularity means that n_l and/or $n_r > 1$. The order zero, that is, n_l resp. $n_r = 0$, means of course that all elements of $\mathfrak{R}$ are right resp. left divisors of zero.

THEOREM. *There exist no rings of finite* (*left or right*) *order* $n > 1$.

PROOF.[4] Assume $\mathfrak{R}$ to be of right order $n_r > 1$. Then there exist at least two lin. r. ind. elements $a, b \in \mathfrak{R}$, that is, $ax+by=0$ implies $x=y=0$. Then the 4 elements aa, ab, ba, bb will also be lin. r. ind., because by using the associativity of multiplication and the right distributive law[3] $aa \cdot x+ab \cdot y+ba \cdot z+bb \cdot t=a(ax+by)+b(az+bt)=0$ implies $ax+by=az+bt=0$ and hence $x=y=z=t=0$. Similarly the 8 elements aaa, aab, $\cdots$, bbb and generally all the 2^n elements, obtained by forming all possible "words" of length n using the 2 "letters" a and b, can be proved to be lin. r. ind. Indeed, if c_i $(i=1, \cdots, \nu=2^{n-1})$ are the above defined products of length $(n-1)$, the 2^n products of length n are given by ac_i, bc_i $(i=1, \cdots, \nu)$. Therefore $\sum ac_i \cdot x_i + \sum bc_i \cdot y_i = a \sum c_i x_i + b \sum c_i y_i = 0$ implies $\sum c_i x_i = \sum c_i y_i = 0$. If we assume the lin. r. independence of the c_i, $x_i = y_i = 0$ is implied and therefore the lin. r. ind. of the 2^n elements ac_i, bc_i is proved by induction. As the same holds for left indep., our theorem is proved.

COROLLARY. *There exist at most the following* 9 *types of rings*:

[3] In view of later developments, it is worth while to note that all these remarks follow either directly from the distributive laws or from their consequences $0 \cdot r = 0$, $r \cdot 0 = 0$, for any $r \in \mathfrak{R}$. $a(b+c)=ab+ac$ is the right distributive law, $(a+b)c=ac+bc$ the left one.

[4] This theorem can also be obtained as a corollary of a more general theory concerning modules with rings as operator domains. Such modules seem to have been considered independently by Paul Dubreil (see Mathematical Reviews vol. 7 (1946) pp. 2, 3).

$(0, 0)$, $(0, 1)$, $(0, \infty)$, $(1, 0)$, $(\infty, 0)$, $(1, 1)$, $(1, \infty)$, $(\infty, 1)$, (∞, ∞).[5]

That rings of each of these types really exist will be shown by examples in §2.

This result permits us to formulate our classification of rings in the following form: $\mathfrak{R}$ is of r. (l.) order 0 only when all its elements are l. (r.) divisors of zero. Otherwise $\mathfrak{R}$ is of r. (l.) order 1 or ∞. It is of r. (l.) order 1 when every pair of elements has a nontrivial C.R.(L.)M. It is of order ∞ when not every pair of elements has a nontrivial C.R.M. In this form we see that our second approach is not much more general than our first. It is also seen that our classification of rings is one of semigroups only, because "divisor of zero" and "common multiple" are notions based on multiplication only. A semigroup, namely, is a system with one composition (multiplication), which is (1) general, (2) unique and (3) associative. It remains only to define "divisors of zero" for a semigroup $\mathfrak{S}$ as follows: $a \in \mathfrak{S}$ is a right (left) *divisor of zero* in $\mathfrak{S}$, if there exists a pair $x, y \in \mathfrak{S}$, $x \neq y$, such that $xa = ya$ $(ax = ay)$.[6] Therefore a is not a r. (l.) divisor of zero, if $xa = ya$ $(ax = ay)$ implies $x = y$. Thus $\mathfrak{S}$ is a semigroup without divisors of zero, right and/or left, if the right and/or left cancellation law (that is, $ba = ca$ and/or $ab = ac$ implies $b = c$) holds in $\mathfrak{S}$. Now if we consider a ring as a semigroup with respect to multiplication the above defined concept of divisor of zero becomes identical with that usually defined for rings.[7]

In this connection it is of interest to point out some differences between semigroups and rings: (1) In a ring with divisors of zero there must exist right as well as left divisors of zero; but in semigroups it may occur that all elements are right divisors of zero (that is, $n_l = 0$) with not a single one being a left divisor of zero. (2) In a ring of order 0, say $n_l = 0$, there exists for every pair of elements at least one nontrivial C.L.M. $= 0$; but in semigroups it may occur that $n_l = 0$ with no C.L.M. whichever existing. (3) As a semigroup

[5] As to rings without divisors of zero, only such of the last type (∞, ∞) are properly irregular in the sense that they can not be immersed in a quotient field according to the construction given in the previously mentioned paper of Ore, while the others permit this construction, which requires regularity on one side only. This does not exclude the immersibility into other kinds of embracing fields. The analogous remark holds for semigroups too.

[6] In the case $\mathfrak{S}$ contains a zero element the latter is called a trivial divisor of zero.

[7] Every divisor of zero in the multiplicative semigroup is also a divisor of zero in the ring and conversely. For trivial ones this is clear. For nontrivial ones this follows by the distributive laws: $ac = bc$, $a \neq b$, $c \neq 0$ implies $(a-b)c = 0$, $a - b \neq 0$, $c \neq 0$. $dc = 0$, $d \neq 0$, $c \neq 0$ implies, for each x, $d((c+x)-x) = 0$ and hence $d(c+x) = dx$, $c + x \neq x$ and, for each y, $((d+y)-y)c = 0$ and hence $(d+y)c = yc$, $d + y \neq y$.

may be finite, but not of order 0 or 1 (for rings this is impossible), it seems more appropriate to use the letter i (to suggest "irregular") instead of the symbol ∞ in the notation for types of semigroups. This is especially necessary in view of a more general theory of "ringlike domains," as will be shown elsewhere.

2. **Examples.** We start by constructing a semigroup without divisors of zero $\mathfrak{F}$ of type (i, i). Any "*word*" composed by the 2 letters x, y shall be an element of $\mathfrak{F}$, and nonidentical "words" represent different elements. The composition, defined by connecting one word to the other, is obviously (1) general, (2) unique, (3) associative, and (4) complies with the cancellation laws. No C.R.(L.)M.'s exist except in the case of one word being a right (left) "end" (that is, "divisor" or "part") of its pair. Therefore $\mathfrak{F}$ is of the required type.

Consider all elements of $\mathfrak{F}$ as the basis of a module $\mathfrak{M}$ over a ring $\mathfrak{R}$, which may be chosen as the field $\{0, 1\}$ of residue classes (mod 2). Thus each nonzero element of $\mathfrak{M}$ has the form $\sum f_i$, where the f_i's form an arbitrary finite set of different elements of $\mathfrak{F}$. Defining multiplication in $\mathfrak{M}$ by the distributive laws, $\mathfrak{M}$ becomes a ring which can be called the "*semigroup ring*" of $\mathfrak{F}$ over $\mathfrak{R}$, written $\mathfrak{R}(\mathfrak{F})$. We call the sums $\sum f_i$ "*polynomials*," those consisting of one term "*monomials*." The "*degree*" of a monomial $f \in \mathfrak{F}, f \in \mathfrak{R}(\mathfrak{F})$ is the number of its letters and is denoted by $\delta(f)$ A polynomial p containing only monomials of equal degree δ is called a "*homogeneous*" polynomial of degree $\delta = \delta(p)$. Any polynomial P is a sum of monomials. P is also a sum of homogeneous polynomials p_i of different degrees, that is, $P = \sum_{i=1}^{n} p_i$ with $\delta(p_1) < \delta(p_2) < \cdots < \delta(p_n) = \delta(P)$, the *degree of* P. By multiplying terms of highest degree $\delta(P)$, $\delta(Q)$ of $P \neq 0$, $Q \neq 0$ we obtain every product of degree $\delta(P)+\delta(Q)$ only once. This yields exactly all terms of highest degree $\delta(PQ)$ in PQ, which therefore cannot vanish, giving the rule $\delta(PQ) = \delta(P)+\delta(Q)$. From this it follows as for ordinary polynomials that our ring $\mathfrak{R}(\mathfrak{F})$ does not contain divisors of zero. $\mathfrak{R}(\mathfrak{F})$ is of the type (∞, ∞): to show this it is enough to find 2 monomials which have neither C.R.M. nor C.L.M. Indeed, by choosing the generators x, y themselves whatever the polynomials $P, Q \in \mathfrak{R}(\mathfrak{F})$, it is obvious that $Px \neq Qy$ $(xP \neq yQ)$, because Px (xP) is composed of monomials ending (beginning) with x only, while all monomials of Qy (yQ) end (begin) with y.

Next we construct a semigroup without divisors of zero $\mathfrak{G}$ of type $(1, i)$ consisting of all symbols $x^\alpha y^\beta$ $(\alpha, \beta = 0, 1, 2, \cdots)$. We define equality and composition by: $x^{\alpha_1}y^{\beta_1} = x^{\alpha_2}y^{\beta_2}$ only when $\alpha_1 = \alpha_2$, $\beta_1 = \beta_2$ and conversely. $x^{\alpha_1}y^{\beta_1} \cdot x^{\alpha_2}y^{\beta_2} = x^{\gamma}y^{\beta_1+\beta_2}$, $\gamma = \alpha_1 + 2^{\beta_1}\alpha_2$. The composition is (1) general, (2) unique, (3) associative, and (4)

complies with the cancellation laws, as may be easily verified.[8] To any 2 elements $g_i = x^{\alpha_i} y^{\beta_i} \in \mathfrak{G}$ $(i = 1, 2)$, we can find 2 elements $z_i = x^{\xi_i} y^{\eta_i}$ $(i = 1, 2)$, such that $z_1 g_1 = z_2 g_2$; for example, if we take $\eta_1 = \beta_2$, $\eta_2 = \beta_1$, $\xi_1 = 2^{\beta_1}\alpha_2$, $\xi_2 = 2^{\beta_2}\alpha_1$, the C.L.M. (g_1, g_2) becomes $x^{\lambda} y^{\beta_1+\beta_2}$ with $\lambda = 2^{\beta_1}\alpha_2 + 2^{\beta_2}\alpha_1$. But generally the g_i have no C.R.M., because $g_i z_i = x^{\alpha_i+\xi_i} y^{\beta_i+\eta_i}$, and because for $\beta_1, \beta_2 \neq 0$ and $\alpha_1 \not\equiv \alpha_2 \pmod 2$ no ξ_i, η_i can be found such that $g_1 z_1 = g_2 z_2$; for example xy and $x^2 y$ certainly have no C.R.M. $\mathfrak{G}$ is therefore of the type $(1, i)$.

Similarly, as before, we construct a semigroup ring $\mathfrak{R}(\mathfrak{G})$ and write the general element $P \in \mathfrak{R}(\mathfrak{G})$ as a polynomial in y using the left distributive law: $P = \sum_{i=0}^{\mu} p_i(x) y^i$, where the p_i are polynomials in x, $p_\mu(x) \neq 0$ and $\mu = \delta_y(P)$, the *"degree of P in y."* Note the multiplication rule: $y^\beta p(x) = p(x^{2^\beta}) y^\beta$. As may be easily verified $\mathfrak{R}(\mathfrak{G})$ does not contain divisors of zero. The monomials xy and $x^2 y$ have no C.R.M. in $\mathfrak{R}(\mathfrak{G})$. Indeed from $xyP = x^2 yQ$ it would follow that the different monomials of xyP are equal in some order to those of $x^2 yQ$, which is impossible. Therefore $n_r = \infty$.

To prove $n_l = 1$ we take advantage of some results contained in O. Ore's paper *Theory of non-commutative polynomials* (Ann. of Math. vol. 34 (1933) pp. 480–508) and consider the ring $\mathfrak{R}^*$ of the noncommutative polynomials $P^* = \sum r_i y^i$ where $r_i = r_i(x) = p_i(x)/p_i'(x)$ are elements of the field of all rational functions of x over $\mathfrak{R}$. The multiplication in $\mathfrak{R}^*$ shall be defined by $yr = \bar{r}y + r' = r(x^2)y$; that is,

$$\overline{r(x)} = r(x^2), \qquad r'(x) = 0.^9$$

Thus we specialize Ore's operations in such a way that $\mathfrak{R}(\mathfrak{G})$ may be identified with a subring of $\mathfrak{R}^*$. We know that for every 2 elements $P, Q \in \mathfrak{R}(\mathfrak{G}) \subset \mathfrak{R}^*$ we can find $S^*, T^* \in \mathfrak{R}^*$, not both 0, such that $S^*P = T^*Q = \text{C.L.M.}\ (P, Q) \in \mathfrak{R}^*$. By left-hand multiplication with a suitable polynomial $p(x)$ we get $pS^* = S$, $pT^* = T$, $S, T \in \mathfrak{R}(\mathfrak{G})$ and therefore $SP = TQ = \text{C.L.M.}(P, Q) \in \mathfrak{R}(\mathfrak{G})$. By the way, the ring $\mathfrak{R}^*$ itself is also of the type $(1, \infty)$. We need only to show that $n_r = \infty$. It is sufficient to prove that, for example, $xy \cdot P^* \neq x^2 y \cdot Q^*$ for every pair $P^*, Q^* \in \mathfrak{R}^*$, not both 0. Indeed, from $xyP^* = x^2 yQ^*$ it would follow that $xy(\sum r_i(x) y^i) = x^2 y(\sum s_i(x) y^i)$, that is, $\sum r_i(x^2) y^{i+1} = x \sum s_i(x^2) y^{i+1}$, that is, $r_i(x^2) = x s_i(x^2)$ and hence, for at least one index i, $x = r_i(x^2)/s_i(x^2) = t(x^2)$, that is, x is a rational function of x^2, which is impossible.

Now we construct a semigroup $\mathfrak{H}$ of type $(0, i)$ by taking all the

[8] The semigroup could also have been defined by the 2 generators x and y and the defining relation $yx = x^2 y$.

[9] Compare loc. cit. p. 481, equation (3).

symbols (words) $f\in\mathfrak{F}$ (see first example) and adding the symbols ϵ and $f\epsilon$ (that is, a word of $\mathfrak{F}$ with an ϵ "hung on"). We define equality by identity and composition by connecting words, with the additional provision that an ϵ not standing at the end (that is, belonging to the first (left) factor) shall be suppressed. In this way we obtain again one and only one symbol of $\mathfrak{H}$, that is, the composition is general and unique; its associativity is obvious too. All elements of $\mathfrak{H}$ are right divisors of zero, because for $f\in\mathfrak{F}\subset\mathfrak{H}$ we have $f\epsilon\neq f$, but $f\epsilon\cdot h=fh$ for every $h\in\mathfrak{H}$. But $\mathfrak{H}$ has no left divisors of zero because $h_1\neq h_2$ implies, for every $h\in\mathfrak{H}$, $hh_1\neq hh_2$. The two special elements $x, y\in\mathfrak{H}$ have no C.R.M. because $xh\neq yh$ for every $h\in\mathfrak{H}$. $\mathfrak{H}$ is therefore indeed of type $(0, i)$.

As in the previous examples we construct the semigroup ring $\mathfrak{R}(\mathfrak{H})$. Its elements have the forms $R=P(x, y)+Q(x, y)\cdot\epsilon=P+Q\epsilon$, where $P, Q\in\mathfrak{R}(\mathfrak{F})$. The multiplication rule is $R_1R_2=(P_1+Q_1\epsilon)(P_2+Q_2\epsilon)$ $=(P_1+Q_1)P_2+(P_1+Q_1)Q_2\epsilon=(P_1+Q_1)R_2$. $R_1R_2=0$, $R_1, R_2\neq 0$ implies $(P_1+Q_1)P_2=(P_1+Q_1)Q_2=0$, that is, $P_1+Q_1=0$, that is, $P_1=Q_1$, that is, $P_1\equiv Q_1 \pmod 2$. Therefore every element $R_2\in\mathfrak{R}(\mathfrak{H})$ is a right divisor of zero, that is, $n_l=0$. But $n_r=\infty$, because the 2 elements $x, y\in\mathfrak{R}(\mathfrak{H})$ have no C.R.M.: $xR_1\neq yR_2$ for any $R_1, R_2\in\mathfrak{R}(\mathfrak{H})$. $\mathfrak{R}(\mathfrak{H})$ is therefore of type $(0, \infty)$.

We consider the semigroup $\mathfrak{J}$ consisting of the symbols ϵ, x^n and $x^n\epsilon$ $(n=1, 2, \cdots)$ with identity and composition defined as for $\mathfrak{H}$. Every element of $\mathfrak{J}$ is a right divisor for zero, but none a left one; any 2 elements have a C.R.M. Therefore $\mathfrak{J}$ is of the required type $(0, 1)$. Considering again the semigroup ring $\mathfrak{R}(\mathfrak{J})$ we see that its elements have the form $R=p(x)+q(x)\epsilon$ with the same multiplication rule as in $\mathfrak{R}(\mathfrak{H})$ and therefore $n_l=0$. But $n_r=1$, because for any $R_i=p_i+q_i\epsilon$ $(i=1, 2)$ we can find $U_i=s_i+t_i\epsilon$ with $R_1U_1=R_2U_2$; for example, choose $t_1=t_2=0$, $s_1=p_2+q_2$, $s_2=p_1+q_1$.

For the type $(0, 0)$ we may construct an example, different from the trivial $\{0\}$ containing the zero element only, by taking any finite or infinite set of different symbols x_i, one of them being "0." This set becomes a semigroup $\mathfrak{J}$ by defining multiplication by $x_ix_j=0$, that is, every product is 0. $\mathfrak{J}$ is of type $(0, 0)$, and so is the semigroup ring $\mathfrak{R}(\mathfrak{J})$, as is easily seen.

Conclusion: As the type $(1, 1)$ is that of the most common rings and as by simple symmetry our examples prove also the existence of rings (semigroups) of the types $(\infty, 1)$, $(\infty, 0)$ (resp. $(i, 1)$, $(i, 0)$) and $(1, 0)$, we have proved that rings and semigroups of every one of the 9 possible types really exist.

HEBREW UNIVERSITY