NEAR-VECTOR SPACES CONSTRUCTED FROM NEAR DOMAINS

K.-T. HOWELL AND S. P. SANON

Abstract. In this paper we prove some new results on near-vector spaces and near domains and give a first application of the nearring of quotients with respect to a multiplicative set, namely we construct a new class of near-vector spaces from near domains.

2010 *Mathematics Subject Classification:* 16Y30; 12K05

Keywords: nearrings of quotients, near-vector spaces, nearrings

1. INTRODUCTION

André [1] first generalised the concept of a vector space, i.e., a linear space, to a structure comprising a bit more non-linearity, the so-called near-vector space. In [12] van der Walt showed how to construct an arbitrary finite-dimensional near-vector space, using a finite number of near-fields, all having isomorphic multiplicative semigroups. This construction was used in [7] to characterise all finite dimensional near-vector spaces over $\mathbb{Z}_p$, for p a prime. These results were extended in [8] to all finite dimensional near-vector spaces over arbitrary finite fields. In [6] homogeneous and linear mappings and subspaces were investigated.

Recently, near-vector spaces have been used in several applications, including in secret sharing schemes in cryptography [4] and to construct interesting examples of families of planar nearrings [3]. In addition, they have proved interesting from a model theory perspective too [2].

In this paper we begin with some preliminary material in section 2.1. on near-vector spaces and prove some properties of isomorphisms of near-vector spaces. In section 2.2. we generalise a construction that was first considered in [6] and in section 2.3. we focus on nearrings of quotients, giving some new results that allow for alternative proofs of some of the main known results. In section 2.4. we focus on

integral nearrings and near domains and prove that if a nearring N is integral, then the nearring of quotients, N_S will be integral and that if N is a near domain and S the set of all cancellable elements of N, then N_S will be a nearfield. Finally, as a first application of nearrings of quotients, in section 2.5. we use the results from section 2.4. to construct a new class of near-vector spaces from near domains.

2. RESULTS

2.1. *Preliminary considerations*

Definition 1 ([1]). A pair (V, A) is called a *near-vector space* if:
  (1) $(V, +)$ is a group and A is a set of endomorphisms of V;
  (2) A contains the endomorphisms 0, *id* and $-id$;
  (3) $A^* = A \setminus \{0\}$ is a subgroup of the group $\mathrm{Aut}(V)$;
  (4) A acts fixed point free (fpf) on V, i.e., for $x \in V, \alpha, \beta \in A$, $x\alpha = x\beta$ implies that $x = 0$ or $\alpha = \beta$;
  (5) the quasi-kernel $Q(V)$ of V, generates V as a group. Here, $Q(V) = \{x \in V \mid \forall \alpha, \beta \in A, \exists \gamma \in A$ such that $x\alpha + x\beta = x\gamma\}$.

We sometimes refer to V as a *near-vector space over A*. The elements of V are called *vectors* and the members of A *scalars*. The action of A on V is called *scalar multiplication*. Note that $-id \in A$ implies that $(V, +)$ is an abelian group. Also, the dimension of the near-vector space, $\dim(V)$, is uniquely determined by the cardinality of an independent generating set for $Q(V)$. See [1] for further details.

In [12] van der Walt proved the following theorem,

Theorem 1 ([12] Theorem 3.4, p.301). *Let V be a group and let $A := D \cup \{0\}$, where D is a fix point free group of automorphisms of V. Then (V, A) is a finite dimensional near-vector space if and only if there exists a finite number of nearfields, $F_1, F_2, \ldots, F_n$, semigroup isomorphisms $\psi_i : A \to F_i$ and a group isomorphism $\Phi : V \to F_1 \oplus F_2 \oplus \cdots \oplus F_n$ such that if*

$$\Phi(v) = (x_1, x_2, \cdots, x_n), \ (x_i \in F_i)$$

then

$$\Phi(v\alpha) = (x_1\psi_1(\alpha), x_2\psi_2(\alpha), \cdots, x_n\psi_n(\alpha)),$$

for all $v \in V$ and $\alpha \in A$.

According to this theorem we can specify a finite dimensional near-vector space by taking n nearfields $F_1, F_2, \ldots, F_n$ for which there are semigroup isomorphisms $\vartheta_{ij} : (F_j, \cdot) \to (F_i, \cdot)$ with $\vartheta_{ij}\vartheta_{jk} = \vartheta_{ik}$ for $1 \leq i, j, k \leq n$. We can then take $V := F_1 \oplus F_2 \oplus \cdots \oplus F_n$ as the additive group of the near-vector space and any one of the semigroups $(F_{i_o}, \cdot)$ as the semigroup of endomorphisms by defining

$$(x_1, x_2, \ldots, x_n)\alpha := (x_1\vartheta_{1i_o}(\alpha), x_2\vartheta_{2i_o}(\alpha), \cdots, x_n\vartheta_{ni_o}(\alpha)),$$

for all $x_j \in F_j$ and all $\alpha \in F_{i_o}$.

Definition 2 ([8] Definition 3.2, p.4)**.** We say that two near-vector spaces (V_1, A_1) and (V_2, A_2) are *isomorphic* (written $(V_1, A_1) \cong (V_2, A_2)$ if there are group isomorphisms $\theta : (V_1, +) \rightarrow (V_2, +)$ and $\eta : (A_1^*, \cdot) \rightarrow (A_2^*, \cdot)$ such that $\theta(x\alpha) = \theta(x)\eta(\alpha)$ for all $x \in V_1$ and $\alpha \in A_1^*$.

We denote this pair by (θ, η). Isomorphisms map quasi-kernels to quasi-kernels:

Proposition 1. *If the near-vector spaces (V_1, A_1) and (V_2, A_2) are isomorphic, then $Q(V_1)$ is mapped to $Q(V_2)$.*

Proof. Let $v \in Q(V_1)$. If $v = 0$, then $\theta(v) \in Q(V_2)$, so suppose that $v \neq 0$. Let $\alpha, \beta \in A_2$, then

$$\begin{aligned}
\theta(v)\alpha + \theta(v)\beta &= \theta(v)\eta(\alpha_1) + \theta(v)\eta(\beta_1) \text{ for some } \alpha_1, \beta_1 \in A_1, \\
&= \theta(v\alpha_1) + \theta(v\beta_1) \\
&= \theta(v\alpha_1 + v\beta_1) \\
&= \theta(v\gamma_1) \text{ for some } \gamma_1 \in A_1, \\
&= \theta(v)\eta(\gamma_1).
\end{aligned}$$

Thus $\theta(v) \in Q(V_2)$. $\square$

It is not difficult to show that

Lemma 1. *If (θ, η) is an isomorphism of (V_1, A_1) onto (V_2, A_2), then θ is uniquely determined on any basis of (V_1, A_1).*

In [1], the concept of regularity is introduced as a central notion. A near-vector space is *regular* if any two vectors of $Q(V) \backslash \{0\}$ are *compatible,* i.e. if for any two vectors u and v of $Q(V)$ there exists a $\lambda \in A \backslash \{0\}$ such that $u + v\lambda \in Q(V)$. Every near-vector space can be uniquely decomposed into a direct sum of regular near-vector spaces V_j ($j \in J$) ([1], Theorem 4.13, p.12) and there is a unique direct decomposition into maximal regular near-vector spaces, called the *canonical decomposition* of V. Thus the theory of near-vector spaces is largely reduced to the theory of regular near-vector spaces.

Theorem 2. *If the near-vector spaces (V_1, A_1) and (V_2, A_2) are isomorphic and (V_1, A_1) is regular, (V_2, A_2) will be regular too, i.e. isomorphisms preserve regularity.*

Proof. By definition there exist group isomorphisms $\theta : (V_1, +) \rightarrow (V_2, +)$ and $\eta : (A_1^*, \cdot) \rightarrow (A_2^*, \cdot)$ such that $\theta(x\alpha) = \theta(x)\eta(\alpha)$ for all $x \in V_1$ and $\alpha \in A_1^*$. Let $w_1, w_2 \in Q(V_2) \backslash \{0\}$. Then there exist $v_1, v_2 \in Q(V_1)$ (by Proposition 1), such that $w_1 = \theta(v_1)$ and $w_2 = \theta(v_2)$. Since V_1 is regular there exists a $\lambda \in A_1^*$ such that $v_1 + v_2\lambda \in Q(V_1)$. Thus

$$\theta(v_1 + v_2\lambda) = \theta(v_1) + \theta(v_2)\eta(\lambda)$$

$$= w_1 + w_2\eta(\lambda) \text{ with } \eta(\lambda) \neq 0.$$

Thus (V_2, A_2) is regular.   □

We also have that

Lemma 2. *Let (V_1, A_1) and (V_2, A_2) be near-vector spaces and (θ, η) an isomorphism. If $V_1 = \bigoplus_{j \in J} V_j$ is the canonical direct decomposition of V_1, then $V_2 = \bigoplus_{j \in J} \theta(V_j)$ is the canonical direct decomposition of V_2.*

The proof is similar to that of Lemma 5.5, p.2537 in [6].

2.2. *Near-vector spaces of the form F^n where F is a nearfield*

In [6] van der Walt's characterisation was used to discuss several constructions of near-vector spaces. In particular, the case where we let $V = F^n$, $n \in \mathbb{N}$, F a nearfield and we take all the isomorphisms to be identical, so that

$$(x_1, x_2, \ldots, x_n)\alpha = (x_1\alpha, x_2\alpha, \ldots, x_n\alpha)$$

was considered.

This is the case closest to the normal vector space setting. Let us denote it by (V, F). In fact, when F is a field, (V, F) is a vector space. We will denote the set of all distributive elements of F by F_d (as in [10]), i.e.

$$F_d = \{d \in F \mid d(x + y) = dx + dy \; \forall x, y \in F\}.$$

It is not difficult to check that F_d is a subfield of F. Note that $0, 1 \in F_d$. It was shown in [6] that $Q(V) = \cup \mathcal{V}_i$, with $\mathcal{V}_i = (d_1, d_2, \ldots, 1, d_{i+1}, \ldots, d_n)F$, with 1 in position i and $d_i \in F_d$, $i \in \{1, \ldots, n\}$ and that (V, F) is a regular near-vector space (Lemma 3.5., p.2531).

We now generalise,

Theorem 3. *Let F be a near-field and $V = F^n$, $n \in \mathbb{N}$ be a near-vector space with the scalar multiplication defined by*

$$(x_1, \ldots, x_n)\alpha = (x_1\zeta(\alpha), \ldots, x_n\zeta(\alpha))$$

where ζ is an automorphism of $(F, \cdot)$ and $\alpha \in F$. Then

$$Q(V) = \{(d_i)\lambda \mid \lambda \in F, d_i \in F_d \text{ for all } i \in I\},$$

where $I = \{1, 2, \ldots, n\}$.

Proof. Let $d_i \in F_d$ for $i \in \{1, \ldots, n\}$ and $\alpha, \beta \in F$. We have

$$\begin{aligned}
(d_i)\alpha + (d_i)\beta &= (d_i\zeta(\alpha) + d_i\zeta(\beta)) \\
&= (d_i(\zeta(\alpha) + \zeta(\beta))) \text{ since } d_i \text{ is distributive,} \\
&= (d_i\zeta(\gamma)) \text{ with } \gamma = \zeta^{-1}(\zeta(\alpha) + \zeta(\beta)), \\
&= (d_i)\gamma.
\end{aligned}$$

Hence $(d_i) \in Q(V)$. Since $Q(V)$ is closed under scalar multiplication we have $Q(V) \supseteq \{(d_i)\lambda | \lambda \in F, d_i \in F_d \text{ for all } i \in I\}$. Now suppose that $(x_i) \in Q(V)$. If $(x_i) = 0$ then $(x_i) \in \{(d_i)\lambda | \lambda \in F, d_i \in F_d \text{ for all } i \in I\}$. Suppose that $(x_i) \neq 0$. Then there is $i_0 \in \{1, \ldots, n\}$ such that $x_{i_0} \neq 0$. Let $d_i = x_i x_{i_0}^{-1}$ for $i \in \{1, \ldots, n\}$. Then $(d_i) = (x_i)\zeta^{-1}(x_{i_0}^{-1})$. Since $(x_i) \in Q(V)$ and $Q(V)$ is closed under scalar multiplication, $(d_i) \in Q(V)$. Then for all $\alpha, \beta \in F$ there is $\gamma \in F$ such that $(d_i)\alpha + (d_i)\beta = (d_i)\gamma$. It follows that $d_i \zeta(\alpha) + d_i \zeta(\beta) = d_i \zeta(\gamma)$ for all $i \in \{1 \ldots, n\}$. Since ζ is an automorphism, there are $\alpha_1, \beta_1 \in F$ such that $\alpha = \zeta^{-1}(\alpha_1)$ and $\beta = \zeta^{-1}(\beta_1)$. So $d_i\alpha_1 + d_i\beta_1 = d_i\zeta(\gamma)$ for all $i \in \{1 \ldots, n\}$. But $d_{i_0} = 1$. So $\alpha_1 + \beta_1 = \zeta(\gamma)$. Hence $d_i\alpha_1 + d_i\beta_1 = d_i(\alpha_1 + \beta_1)$, and this is verified for all $\alpha_1, \beta_1 \in F$ because ζ is an automorphism of $(F, \cdot)$. Therefore d_i is distributive and $Q(V) = \{(d_i)\lambda | \lambda \in F, d_i \in F_d \text{ for all } i \in I\}$. $\square$

In fact, if we take $V = F^n$, $n \in \mathbb{N}$ with F a near-field and denote the near-vector space in the above theorem by (V, F'), we can show that

Proposition 2. *The near-vector spaces (V, F) and (V, F') are isomorphic for the same nearfield F.*

Proof. Using Definition 2, consider θ the identity isomorphism and $\eta : (F^*, \cdot) \to (F^*, \cdot)$ the mapping $\eta(\alpha) = \zeta^{-1}(\alpha)$. Since ζ is an isomorphism, ζ^{-1} exists and η is an isomorphism. Thus $\theta(x\alpha) = \theta(x)\eta(\alpha)$ for all $x \in V$ and $\alpha \in F^*$. $\square$

Finally, since by Theorem 2 isomorphisms preserve regularity, we have that

Lemma 3. (V, F') *is a regular near-vector space.*

We end off the section with an example,

Example 1. Consider the field $(GF(3^2), +, \cdot)$ with

$$GF(3^2) := \{0, 1, 2, \gamma, 1 + \gamma, 2 + \gamma, 2\gamma, 1 + 2\gamma, 2 + 2\gamma\},$$

where γ is a zero of $x^2 + 1 \in \mathbb{Z}_3[x]$.
The operations on $GF(3^2)$ can be defined as follows:

$$+ : (a + b\gamma) + (c + d\gamma) = (a + c)\text{mod3} + ((b + d)\text{mod3})\gamma,$$

$\cdot$	0	1	2	γ	$1+\gamma$	$2+\gamma$	2γ	$1+2\gamma$	$2+2\gamma$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	γ	$1+\gamma$	$2+\gamma$	2γ	$1+2\gamma$	$2+2\gamma$
2	0	2	1	2γ	$2+2\gamma$	$1+2\gamma$	γ	$2+\gamma$	$1+\gamma$
γ	0	γ	2γ	2	$2+\gamma$	$2+2\gamma$	1	$1+\gamma$	$1+2\gamma$
$1+\gamma$	0	$1+\gamma$	$2+2\gamma$	$2+\gamma$	2γ	1	$1+2\gamma$	2	γ
$2+\gamma$	0	$2+\gamma$	$1+2\gamma$	$2+2\gamma$	1	γ	$1+\gamma$	2γ	2
2γ	0	2γ	γ	1	$1+2\gamma$	$1+\gamma$	2	$2+2\gamma$	$2+\gamma$
$1+2\gamma$	0	$1+2\gamma$	$2+\gamma$	$1+\gamma$	2	2γ	$2+2\gamma$	γ	1
$2+2\gamma$	0	$2+2\gamma$	$1+\gamma$	$1+2\gamma$	γ	2	$2+\gamma$	1	2γ

In [11], p.257, it is observed that $(GF(3^2), +, \circ)$, with

$$x \circ y := \begin{cases} x \cdot y & \text{if } y \text{ is a square in } (GF(3^2), +, \cdot) \\ x^3 \cdot y & \text{otherwise} \end{cases}$$

is a (right) nearfield, but not a field.

$\circ$	0	1	2	γ	$1+\gamma$	$2+\gamma$	2γ	$1+2\gamma$	$2+2\gamma$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	γ	$1+\gamma$	$2+\gamma$	2γ	$1+2\gamma$	$2+2\gamma$
2	0	2	1	2γ	$2+2\gamma$	$1+2\gamma$	γ	$2+\gamma$	$1+\gamma$
γ	0	γ	2γ	2	$1+2\gamma$	$1+\gamma$	1	$2+2\gamma$	$2+\gamma$
$1+\gamma$	0	$1+\gamma$	$2+2\gamma$	$2+\gamma$	2	2γ	$1+2\gamma$	γ	1
$2+\gamma$	0	$2+\gamma$	$1+2\gamma$	$2+2\gamma$	γ	2	$1+\gamma$	1	2γ
2γ	0	2γ	γ	1	$2+\gamma$	$2+2\gamma$	2	$1+\gamma$	$1+2\gamma$
$1+2\gamma$	0	$1+2\gamma$	$2+\gamma$	$1+\gamma$	2γ	1	$2+2\gamma$	2	γ
$2+2\gamma$	0	$2+2\gamma$	$1+\gamma$	$1+2\gamma$	1	γ	$2+\gamma$	2γ	2

It is not difficult to see that the the distributive elements of $(GF(3^2), +, \circ)$, denoted by $(GF(3^2), +, \circ)_d$ are the elements $0, 1, 2$. Consider the near-field $F = (GF(3^2, +, \circ)$, put $V = F^3$ with $\alpha \in F$ acting as an endomorphism of V by defining $(x_1, x_2, x_3)\alpha = (x_1\alpha^3, x_2\alpha^3, x_3\alpha^3)$. Thus we have that $Q(V) = \{(d_1, d_2, d_3)\lambda | \lambda \in F, d_i \in \{0, 1, 2\}\}$ and this near-vector space is regular.

2.3. *Nearrings of quotients*

The concept of nearrings of quotients was first defined by Maxson [9] and he stated conditions for a nearring to have a nearring of quotients. Graves and Malone [5] subsequently generalised this to the case of nearrings of quotients with respect to a multiplicative set.

We consider the case where N is a non-commutative nearring and begin with the basic results as found in [5,11]. Corollary 1 and 2 are new results that we use to give alternative proofs to the known results of Theorem 4 and Theorem 5 (See [11]). For more on nearrings we refer the reader to [10,11].

Definition 3 ([11] Definition 6.3, p.26)**.** Let N be a nearring and S a subsemigroup of $(N, \cdot)$. A nearring N_s is called a nearring of right quotients of N with respect to S if

   (1) N_s is a nearring with identity,
   (2) N is embeddable in N_s, by a homomorphism, say h,
   (3) $\forall s \in S$, $h(s)$ is invertible in $(N_s, \cdot)$,
   (4) for all $q \in N_s$, there exists $s \in S$ and $n \in N$ such that $q = h(n)h(s)^{-1}$.

We can also define a nearring of left quotients of N with respect to S, which has the same definition as above, except property 4 which becomes :

   4'. for all $q \in N_s$, there exists $s \in S$ and $n \in N$ such that $q = h(s)^{-1}h(n)$.

It is not difficult to see that any element of N_s can be written as $h(n)h(s)^{-1}$, for $s \in S$ and $n \in N$.

Definition 4 ([11] Definition 6.4, p.26). Let N be a nearring and S a subsemigroup of $(N, \cdot)$. N is said to fulfill the right Ore condition with respect to S, if for all $(n, s) \in N \times S$, there exists $(n_1, s_1) \in N \times S$ such that $ns_1 = sn_1$. Likewise, N is said to fulfill the left Ore condition with respect to S if for all $(n, s) \in N \times S$, there exists $(n_1, s_1) \in N \times S$ such that $s_1 n = n_1 s$.

If N is a nearring and S, a subsemigroup of $(N, \cdot)$ and if for all $s \in S$, s is cancellable (both sides) and N satisfies the right Ore condition with respect to S, then the relation $\sim$ defined on $N \times S$ by

$(n, s) \sim (n', s')$ if $\exists (n_1, s_1) \in N$ such that $ss_1 = s'n_1$ implies that $ns_1 = n'n_1$

is an equivalence relation. Moreover, on the equivalence class of $(n, s) \in N \times S$, denoted by $\frac{n}{s}$, we define the operations $" + "$ and $" \cdot "$ by

$$\frac{n}{s} + \frac{n'}{s'} = \frac{ns_1 + n'n_1}{ss_1} \quad \text{and}$$

$$\frac{n}{s} \cdot \frac{n'}{s'} = \frac{nn_2}{s's_2},$$

where $(n_1, s_1) \in N \times S$ and $(n_2, s_2) \in N \times S$ fulfill $s'n_1 = ss_1$ and $n's_2 = sn_2$. These operations are well-defined and $(N_s = N \times S / \sim, +, \cdot)$ is a nearring of right quotients of N with respect to S.

We prove a new result:

Corollary 1. *Let N_s be a nearring of right quotients of N with respect to S. Then $h(n)h(s)^{-1} = h(n')h(s')^{-1}$ if and only if $(n, s) \sim (n', s')$ for all (n, s) and (n', s') in $N \times S$.*

Proof. Let $(n, s), (n', s') \in N \times S$ such that $(n, s) \sim (n', s')$. Then there exists $(n_1, s_1) \in N \times S$ such that $ss_1 = s'n_1$ implies $ns_1 = n'n_1$. It follows that

$$h(s)h(s_1) = h(s')h(n_1)$$
$$h(n)h(s_1) = h(n')h(n_1).$$

So, since for all $s \in S$, $h(s)$ is invertible in N_s,

$$h(n_1) = h(s')^{-1}h(s)h(s_1)$$
$$h(n) = h(n')h(n_1)h(s_1)^{-1}.$$

Therefore

$$h(n) = h(n')h(s')^{-1}h(s)h(s_1)h(s_1)^{-1}$$
$$= h(n')h(s')^{-1}h(s).$$

Thus $h(n)h(s)^{-1} = h(n')h(s')^{-1}$.

Now we show the converse. Let $(n, s), (n', s') \in N \times S$ such that $h(n)h(s)^{-1} = h(n')h(s')^{-1}$. Then there exists $(n_1, s_1) \in N \times S$ such that $h(s')^{-1}h(s) = h(n_1)h(s_1)^{-1}$, by property 4 in the definition of a nearring of right quotients with respect to S. So $h(ss_1) = h(s'n_1)$. Since h is a monomorphism, $ss_1 = s'n_1$. Also, since $h(s)h(s_1) = h(s')h(n_1)$, $h(s')^{-1}h(s)h(s_1) = h(n_1)$. So $h(s')^{-1} = h(n_1)h(s_1)^{-1}h(s)^{-1}$. Using the fact that $h(n)h(s)^{-1} = h(n')h(s')^{-1}$, we get $h(n)h(s)^{-1} = h(n')h(n_1)h(s_1)^{-1}h(s)^{-1}$. So $h(n)h(s_1) = h(n')h(n_1)$. Therefore $h(ns_1) = h(n'n_1)$ and $ns_1 = n'n_1$, since h is a monomorphism. Thus $(n, s) \sim (n', s')$. $\square$

The use of this corollary allows us to give an alternate proof to that found in [11], of the following theorem:

Theorem 4 ([11] Theorem 1.65, p.27). *Let N be a nearring and S a subsemigroup of $(N, \cdot)$. N has a nearring of right quotients with respect to S is equivalent to*

(1) *for all $s \in S$, s is cancellable (on both sides),*
(2) *N satisfies the right Ore condition with respect to S.*

Proof. Let S be a subsemigroup of $(N, \cdot)$. Suppose that N has a nearring N_s of right quotients with respect to S. So N is embeddable in N_s, by a homomorphism h. Since S is a subsemigroup, $S \neq \varnothing$. Let $s \in S$ and $n, n' \in N$, such that $n's = ns$. Then $h(n')h(s) = h(n)h(s)$. Since $h(s)$ is invertible in $(N_s, \cdot)$, $h(n') = h(n)$. It follows that $n' = n$, since h is a monomorphism. Also if $sn' = sn$, we have $n' = n$. Thus for all $s \in S$, s is cancellable on both sides. Now, let $n \in N$ and $s \in S$. Then $h(s)^{-1}h(n) \in N_s$. So by property 4 of Definition 3, there exists $(s_1, n_1) \in S \times N$, such that $h(s)^{-1}h(n) = h(n_1)h(s_1)^{-1}$. Hence $h(ns_1) = h(sn_1)$, and $ns_1 = sn_1$. Therefore N satisfies the right Ore condition with respect to S.

To show the converse, we suppose that S is not empty, for all $s \in S$, s is cancellable (on both sides) and that N satisfies the right Ore condition with respect to S. So from the discussion following Definition 4 there exists a nearring of right quotients of N with respect to S, namely $(N \times S/\sim, +, \cdot)$. $\square$

Remark 1. We note that there is a printing error in the statement of the above theorem in [11](Theorem 1.65, p.27), the left Ore condition should be replaced with the right Ore condition.

Example 2. Let us consider the nearring $(M(\mathbb{R}), +, \circ)$. An element $f \in M(\mathbb{R})$ is cancellable if and only if f is bijective. In fact if f is bijective, then f is cancellable. So let us suppose f is cancellable. That implies that for all $g, g' \in M(\mathbb{R})$, $f \circ g = f \circ g'$ implies $g = g'$, also $g \circ f = g' \circ f$ implies $g = g'$. It is not difficult to see that $f \circ g = f \circ g'$ implies $g = g'$, implies that f is injective. Also if $g \circ f = g' \circ f$ implies $g = g'$, then f is surjective.

So now let us consider $N = (\mathbb{R}[x], +, \circ) \subset M(\mathbb{R})$, the set of polynomials defined from $\mathbb{R}^+$, and S the set of all monomials in N with co-domain in $\mathbb{R}^+$ (in other words monomials of the form ax^n, with $a \geqslant 0$ and $n \in \mathbb{N}$). Since each monomial is defined on $\mathbb{R}^+$, every element of S is bijective, then cancellable. Also the composition of two monomials is a monomial. Thus S is a subsemigroup of $(N, \circ)$. Moreover for $(f, g) \in N \times S$, $f \circ id = g \circ (g^{-1} \circ f)$. But $(g^{-1} \circ f, id) \in N \times S$, so N satisfies the right Ore condition with respect to S. Hence N has a nearring of right quotients with respect to S.

The quotient is a set $(N_s, +, \circ)$, where N_s is the set of all summations of all power functions $f(x) = x^\alpha$, with $\alpha \in \mathbb{Q}^+$ and f defined from $\mathbb{R}^+$ to $\mathbb{R}$.

We prove a new corollary:

Corollary 2. *Let N be a nearring and S a subsemigroup of $(N, \cdot)$. If N has a nearring of right quotients with respect to S, N_s, then there exists $(n_1, s_1) \in N \times S$ such that $h(n)h(s)^{-1} + h(n')h(s')^{-1} = h(ns_1 + n'n_1)h(ss_1)^{-1}$, where $ss_1 = s'n_1$ and h is the embedding homomorphism from N to N_s. Also, there exists $(n_2, s_2) \in N \times S$ such that $h(n)h(s)^{-1}h(n')h(s')^{-1} = h(nn_2)h(s's_2)^{-1}$, where $n's_2 = sn_2$.*

Proof. Since N has a nearring of right quotients with respect to S, N satisfies the right Ore condition with respect to S. So there exists $(n_1, s_1) \in N \times S$ such that $ss_1 = s'n_1$. Then $h(s')^{-1} = h(n_1)h(s_1)^{-1}h(s)^{-1}$. We have

$$h(ns_1 + n'n_1)h(ss_1)^{-1} = h(n)h(s_1)h(s_1)^{-1}h(s)^{-1} + h(n')h(n_1)h(s_1)^{-1}h(s)^{-1}.$$

Hence $h(ns_1 + n'n_1)h(ss_1)^{-1} = h(n)h(s)^{-1} + h(n')h(s')^{-1}$.
Also, since $(n', s) \in N \times S$, there exists $(n_2, s_2) \in N \times S$ such that $n's_2 = sn_2$, by the right Ore condition. So $h(n_2) = h(s)^{-1}h(n')h(s_2)$.
We have

$$h(nn_2)h(s's_2)^{-1} = h(n)h(n_2)h(s_2)^{-1}h(s')^{-1}$$
$$= h(n)h(s)^{-1}h(n')h(s_2)h(s_2)^{-1}h(s')^{-1}.$$

Hence $h(nn_2)h(s's_2)^{-1} = h(n)h(s)^{-1}h(n')h(s')^{-1}$. □

We will use the above corollary to give an alternate proof of the following result found in [11]:

Theorem 5 ([11] Theorem 1.66, p.28). *Let N be a nearring. If N_s and N'_s are nearrings of right quotients with respect to S, then*

$$N_s \cong N'_s.$$

Proof. Since N_s and N'_s are nearrings of right quotients, there exist monomorphisms h and h', from N to N_s and N to N'_s, respectively. Let us define the mapping f

by

$$f : N_s \rightarrow N_s'$$
$$h(n)h(s)^{-1} \mapsto h'(n)h'(s)^{-1}.$$

The mapping f is well-defined. To show this suppose that $h(n)h(s)^{-1} = h(n')h(s')^{-1}$. Then by Corollary 1 $(n,s) \sim (n',s')$. Also by the same Corollary 1 $h'(n)h'(s)^{-1} = h'(n')h'(s')^{-1}$. So $f(h(n)h(s)^{-1}) = f(h(n')h(s')^{-1})$. Thus f is well-defined. Let $h(n)h(s)^{-1}, h(n')h(s')^{-1} \in N_s$. Then by Corollary 2 we have

$$f(h(n)h(s)^{-1} + h(n')h(s')^{-1}) = f(h(ns_1 + n'n_1)h(ss_1)^{-1}) \ (n_1,s_1) \in N \times S$$
$$\text{fulfilling } s'n_1 = ss_1$$
$$= h'(ns_1 + n'n_1)h'(ss_1)^{-1}$$
$$= h'(n)h'(s)^{-1} + h'(n')h'(s')^{-1} \text{ since } s'n_1 = ss_1$$
$$= f(h(n)h(s)^{-1}) + f(h(n')h(s')^{-1}).$$

Also by Corollary 2 again, we have

$$f(h(n)h(s)^{-1}h(n')h(s')^{-1}) = f(h(nn_2)h(s's_2)^{-1}), \text{ where } (n_2,s_2) \in N \times S$$
$$\text{fulfills } n's_2 = sn_2$$
$$= h'(nn_2)h'(s's_2)^{-1}$$
$$= h'(n)h'(s)^{-1}h'(n')h'(s')^{-1}, \text{ since } n's_2 = sn_2$$
$$= f(h(n)h(s)^{-1})f(h(n')h(s')^{-1}).$$

Thus f is a homomorphism. Now, let $h(n)h(s)^{-1}, h(n')h(s')^{-1} \in N_s$ such that $h'(n)h'(s)^{-1} = h'(n')h'(s')^{-1}$. Then $(s,n) \sim (s',n')$. So $h(n)h(s)^{-1} = h(n')h(s')^{-1}$. Hence f is injective. Let $h'(n)h'(s)^{-1} \in N_s'$. For $(n,s) \in N \times S$, $h(n)h(s)^{-1} \in N_s$ and $f(h(n)h(s)^{-1}) = h'(n)h'(s)^{-1}$. Hence f is a surjection. Therefore f is a bijection. Thus $N_s \cong N_s'$. $\qquad\square$

Theorem 5 allow us to speak of the nearring of right quotients, N_s, with respect to S, for a particular nearring.

2.4. *Integral nearrings and near domains*

Recall that a nearring $(N, +, \cdot)$ is said to be *integral* if it has no non-zero divisors of zero and

Definition 5. ([5] Definition 1.4, p.34) A near domain is a nearring N that satisfies the right Ore condition and the left cancellation law.

Then we have the following:

Theorem 6. *Let N be a nearring and S a subsemigroup of $(N, \cdot)$. Suppose that N has a nearring of right quotients with respect to S, N_s. If N is integral, then N_s is integral.*

Proof. Let $h(n)h(s)^{-1}, h(n')h(s')^{-1} \in N_s$ with h the monomorphism from N to N_s. We have

$$h(n)h(s)^{-1}h(n')h(s')^{-1} = h(nn_2)h(s's_2)^{-1},$$

$$\text{with } sn_2 = n's_2 \text{ for } (n_2, s_2) \in N \times S.$$

Suppose that $h(nn_2)h(s's_2) = 0$. Then $h(nn_2)h(s's_2)^{-1} = h(0)h(t)^{-1}$, for some $t \in S$. This implies that $(nn_2, s's_2) \sim (0, t)$. It follows that there exits $(n_1, s_1) \in N \times S$ such that $nn_2s_2 = 0$. $s_2 \neq 0$ because $h(s_2)$ is invertible. Hence $nn_2 = 0$, since N is integral. Moreover, since N is integral, $n = 0$ or $n_2 = 0$. $n_2 = 0$ implies that $n's_2 = 0$ and so $n' = 0$. Therefore $n = 0$ or $n' = 0$. Thus $h(n)(s)^{-1} = 0$ or $h(n')h(s')^{-1} = 0$. Thus N_s is integral. $\square$

Proposition 3. *Let N be a near domain. Then*

(1) $0n = n0 = 0$, *for all $n \in N$*
(2) *N is integral*
(3) *N satisfies the right cancellation law.*

Proof. Let N be a near domain and $n, n_1, n_2 \in N$.

(1) It is straightforward to show that $0n = 0$. We have $(n0)(n0) = n(0n)0 = n0$. So $(n0)(n0)0 = (n0)0$. Using the left cancellation law we have $n0 = 0$.
(2) Suppose $n_1n_2 = 0$. If $n_1 \neq 0$ we have $n_1n_2 = n_10$. It follows that $n_2 = 0$ from the left cancellation law.
(3) If $n_1n = n_2n$, with $n \neq 0$, then $(n_1 - n_2)n = 0$. Hence by 2. $n_1 = n_2$.

$\square$

Corollary 3. *Let N be a near domain. Let S be the set of all cancellable elements of N. Then N_s is a nearfield.*

Proof.
Since N is a near domain, every non-zero element is cancellable. So $S = N - \{0\}$. We know from Definition 3 that $h(s)$ is invertible for every $s \in S$. Let $q \in N_s$. Then there exist $(n, s) \in N \times S$ such that $q = h(n)h(s)^{-1}$. Suppose $q \neq 0$. Then $n \neq 0$. So $n \in S$. Hence $h(n)$ is invertible. Therefore $h(n)h(s)^{-1}$ is invertible and its inverse is $h(s)h(n)^{-1}$. $\square$

2.5. *An application to Near-vector spaces*

In this last section we use the results of the previous sections to give a first application of the theory of nearrings of quotients. We construct a new class of near-vector spaces from near domains and completely describe the quasi-kernel.

If N is a nearfield and $S = N - \{0\}$, then N_s is a nearfield. In fact, we can show that $N \simeq N_s$. From the definition of a nearring of quotients we know that there is an embedding map h defined by

$$h : N \to N_s$$
$$n \mapsto \frac{n}{1}$$

with 1 the multiplicative identity of N. We just have to show that h is surjective. Let $(n, s) \in N \times S$. We have that $\frac{n}{s} = \frac{ns^{-1}}{1}$. So $h(ns^{-1}) = \frac{n}{s}$. Hence h is an isomorphism and so $N \simeq N_s$. Therefore $q = h(n) \in N_s$ is distributive if and only if n is distributive.

Thus if N is a nearfield then

$$N_s \oplus \ldots \oplus N_s \simeq N \oplus \ldots \oplus N$$

and the study of constructions of the form $N \oplus \ldots \oplus N$ has been discussed in [6].

We now look at the case where N is a near domain, not necessarily a nearfield. Let us consider N_s (with identity 1) with S the set of all cancellable elements. We take $V = N_s \bigoplus \ldots \bigoplus N_s$ with the scalar multiplication defined for $(x_1, \ldots, x_n) \in V$ and $\alpha \in N_s$ by

$$(x_1, \ldots, x_n)\alpha = (x_1\alpha, \ldots, x_n\alpha).$$

We now look at the quasi-kernel $Q(V)$. We know from [6] that the quasi-kernel $Q(V) = \mathcal{V}_1 \cup \ldots \cup \mathcal{V}_n$, where $\mathcal{V}_i = \{(d_1, \ldots, d_{i-1}, 1, d_{i+1}, \ldots, d_n)N_s \mid d_i \in N_{sd}\}$, with N_{sd} representing the distributive elements of N_s. Thus in order to describe $Q(V)$, we need to find the elements of N_{sd}.

Theorem 7. $N_{sd} = \{h(n)h(s)^{-1} \mid$ *if* $\exists a, b, c \in N$, *such that* $sa + sb = sc$, *then* $na + nb = nc$ *for* $s \in S$, $n \in N\}$

Proof.
Let $q = h(n)h(s)^{-1}, q_1 = h(n_1)h(s_1)^{-1}, q_2 = h(n_2)h(s_2)^{-1} \in N_s$. First suppose that q is distributive and that there are $a, b, c \in N$ such that $sa + sb = sc$. We prove that $na + nb = nc$. We have

$$h(n)h(s)^{-1}(h(sa + sb)) = h(n)h(s)^{-1}(h(sc)).$$

But

$$h(n)h(s)^{-1}(h(sa + sb)) = h(n)h(s)^{-1}(h(s)h(a) + h(s)h(b))$$
$$= h(n)h(a) + h(n)h(b), \text{ since } h(n)h(s)^{-1} \text{ is distributive.}$$
$$= h(na + nb),$$

and

$$h(n)h(s)^{-1}(h(sc)) = h(nc).$$

Hence, since h is injective, $na + nb = nc$. To show the converse, suppose that if there exist $a, b, c \in N$ such that $sa + sb = sc$, then $na + nb = nc$. We have to prove

that $h(n)h(s)^{-1}$ is distributive in N_s. So we have to show $q(q_1 + q_2) = qq_1 + qq_2$.
We have

$$q(q_1 + q_2) = h(n)h(s)^{-1}h(n_1s^* + n_2n^*)h(s_1s^*)^{-1} \text{ where } s_1s^* = s_2n^*$$
$$= h(nn_1^*)h(s_1s^*s_1^*)^{-1} \text{ where } sn_1^* = (n_1s^* + n_2n^*)s_1^*,$$

and

$$qq_1 + qq_2 = h(nn^{*'})h(s_1s^{*'})^{-1} + h(nn_1^{*'})h(s_2s_1^{*'})^{-1}$$
$$\text{where } sn^{*'} = n_1s^{*'}, sn_1^{*'} = n_2s_1^{*'}$$
$$= h(nn^{*'}s_2^{*'} + nn_1^{*'}n_2^{*'})h(s_1s^{*'}s_2^{*'})^{-1} \text{ where } s_1s^{*'}s_2^{*'} = s_2s_1^{*'}n_2^{*'}.$$

To show that $h(nn_1^*)h(s_1s^*s_1^*)^{-1} = h(nn^{*'}s_2^{*'} + nn_1^{*'}n_2^{*'})h(s_1s^{*'}s_2^{*'})^{-1}$, we have to
find $(n_*^*, s_*^*) \in N \times S$ such that $s_1s^*s_1^*s_*^* = s_1s^{*'}s_2^{*'}n_*^*$ implies $nn_1^*s_*^* = (nn^{*'}s_2^{*'} + nn_1^{*'}n_2^{*'})n_*^*$. Since N_s is a nearring of right quotients with respect to S, we have the
right Ore condition with respect to S. Thus, since $s_1s^*s_1^* \in N, s_1s^{*'}s_2^{*'} \in S$, there
exist $(n_*^*, s_*^*) \in N \times S$ such that $s_1s^*s_1^*s_*^* = s_1s^{*'}s_2^{*'}n_*^*$. But $s_1s^*s_1^*s_*^* = s_1s^{*'}s_2^{*'}n_*^*$
implies $s_2n^*s_1^*s_*^* = s_2s_1^{*'}n_2^{*'}n_*^*$, because $s_1s^{*'}s_2^{*'} = s_2s_1^{*'}n_2^{*'}$ and $s_1s^* = s_2n^*$. So
we get $s^*s_1^*s_*^* = s^{*'}s_2^{*'}n_*^*$ and $n^*s_1^*s_*^* = s_1^{*'}n_2^{*'}n_*^*$, since s_1 and s_2 are cancellable.
Also we have

$$sn^{*'}s_2^{*'}n_*^* = n_1s^{*'}s_2^{*'}n_*^*, \text{ since } sn^{*'} = n_1s^{*'}$$
$$= n_1s^*s_1^*s_*^*, \text{ since } s^*s_1^*s_*^* = s^{*'}s_2^{*'}n_*^*$$

and

$$sn_1^{*'}n_2^{*'}n_*^* = n_2s_1^{*'}n_2^{*'}n_*^*, \text{ since } sn_1^{*'} = n_2s_1^{*'}$$
$$= n_2n^*s_1^*s_*^*, \text{ since } n^*s_1^*s_*^* = s_1^{*'}n_2^{*'}n_*^*.$$

So we get

$$sn^{*'}s_2^{*'}n_*^* + sn_1^{*'}n_2^{*'}n_*^* = n_1s^*s_1^*s_*^* + n_2n^*s_1^*s_*^*$$
$$= (n_1s^* + n_2n^*)s_1^*s_*^*$$
$$= sn_1^*s_*^*, \text{ since } sn_1^* = (n_1s^* + n_2n^*)s_1^*.$$

Hence $s_1s^*s_1^*s_*^* = s_1s^{*'}s_2^{*'}n_*^*$ implies $sn^{*'}s_2^{*'}n_*^* + sn_1^{*'}n_2^{*'}n_*^* = sn_1^*s_*^*$. If we take
$a = n^{*'}s_2^{*'}n_*^*, b = n_1^{*'}n_2^{*'}n_*^*, c = n_1^*s_*^*$, from our assumption we have $na + nb = nc$.
So $nn^{*'}s_2^{*'}n_*^* + nn_1^{*'}n_2^{*'}n_*^* = nn_1^*s_*^*$. Therefore $h(nn_1^*)h(s_1s^*s_1^*)^{-1} = h(nn^{*'}s_2^{*'} + nn_1^{*'}n_2^{*'})h(s_1s^{*'}s_2^{*'})^{-1}$. Thus $h(n)h(s)^{-1}$ is distributive. $\square$

Using Theorem 7 we can describe the quasi-kernel $Q(V)$ of the near vector space
V defined above just by considering the elements of N. So we can construct a near
vector space over a nearfield from a near domain.

In closing we can now describe $Q(V)$ for the above near-vector space.

Corollary 4. *Let us consider the near vector space V defined above, and let $N_1 = \{(n,s) \in N \times N^* \mid if \exists a,b,c \in N, \text{ such that } sa + sb = sc, \text{ then } na + nb = nc \text{ for } s \in S, n \in N\}$. Then we have*

$$Q = \mathcal{V}_1 \cup \ldots \cup \mathcal{V}_n,$$

where

$$\mathcal{V}_i = \{(d_1, \ldots, d_{i-1}, 1, d_{i+1}, \ldots, d_n) N_s \mid d_i = h(n_i) h(s_i)^{-1}, (n,s) \in N_1\}.$$

Moreover, by Lemma 3.5 [6], this near-vector space is regular.

ACKNOWLEDGEMENT

REFERENCES

[1] J. André, "Projektive Ebenen über Fastkörpern," *Math. Z.*, vol. 62, pp. 137–160, 1955.

[2] G. Boxall, K.-T. Howell, and C. Kestner, "Model theory and the construction of near vector spaces," to be submitted 2017.

[3] T. Boykett, "Distribution and generalized center in planar nearrings," submitted 2016.

[4] E. F. Brickell and D. M. Davenport, "On the classification of ideal secret sharing schemes," *Journal of Cryptology*, vol. 4, no. 2, pp. 123–134, 1991.

[5] J. A. Graves and J. J. Malone, "Embedding near domains," *Bulletin of the Australian Mathematical Society*, vol. 9, no. 01, pp. 33–42, 1973.

[6] K.-T. Howell, "On subspaces and mappings of near-vector spaces," *Communications in Algebra*, vol. 43, no. 6, pp. 2524–2540, 2015, doi: 10.1080/00927872.2014.900689. [Online]. Available: http://dx.doi.org/10.1080/00927872.2014.900689

[7] K.-T. Howell and J. H. Meyer, "Finite-dimensional near-vector spaces over fields of prime order," *Comm. Algebra*, vol. 38, no. 1, pp. 86–93, 2010, doi: 10.1080/00927870902855549. [Online]. Available: http://dx.doi.org/10.1080/00927870902855549

[8] K.-T. Howell and J. H. Meyer, "Near-vector spaces determined by finite fields," *J. Algebra*, vol. 398, pp. 55–62, 2014, doi: 10.1016/j.jalgebra.2013.09.019. [Online]. Available: http://dx.doi.org/10.1016/j.jalgebra.2013.09.019

[9] C. J. Maxon, *On near-rings and near-ring modules.* University Microfilms, 1969.

[10] J. D. Meldrum, *Near rings and their links with groups.* Pitman Advanced Publishing Program, 1985, no. 134.

[11] G. Pilz, *Near-rings*, 2nd ed., ser. North-Holland Mathematics Studies. North-Holland Publishing Co., Amsterdam, 1983, vol. 23, the theory and its applications.

[12] A. P. J. van der Walt, "Matrix near-rings contained in 2-primitive near-rings with minimal subgroups," *J. Algebra*, vol. 148, no. 2, pp. 296–304, 1992, doi: 10.1016/0021-8693(92)90195-R. [Online]. Available: http://dx.doi.org/10.1016/0021-8693(92)90195-R

Authors' addresses

K.-T. Howell
Stellenbosch University, Department of Mathematical Sciences, Stellenbosch, South Africa
E-mail address: kthowell@sun.ac.za

S. P. Sanon
Stellenbosch University, Department of Mathematical Sciences, Stellenbosch, South Africa
E-mail address: sogos@sun.ac.za