Quasigroups and Related Systems **6** (1999), 13 – 22

Free R-n-modules

Lăcrimioara Iancu

Abstract

We define the canonical presentation of an R-n-module, in terms of its largest n-submodule with zero and of an idempotent commutative n-group. We give a construction for the free R-n-module with zero, as well as a canonical presentation for the free R-n-module. We give the number of zero-idempotents of a finitely generated free R-n-module. The last theorem states that, for $n \geqslant 3$, free R-n-modules are isomorphic if and only if their free generating sets have the same cardinality.

1. Notations and preliminary results

In [1], N. Celakoski has defined n-modules as a natural generalization of the usual binary notion; however, for his further results he imposed a strong restriction, namely that the commutative n-group involved has a *unique* neutral element. In [4] we restart the study of n-modules by dropping this restriction.

In this section we shall briefly recall some of the definitions and results in [4] and we shall make some additional comments. We use the following conventional notation: the sequence $a_i, \ldots, a_j$ of $j-i+1$ terms of an n-ary sum is denoted by a_i^j and if $a_i = a_{i+1} = \ldots = a_j = a$ then the sequence is denoted by $\overset{(j-i+1)}{a}$; if $i > j$, then a_i^j denotes an empty sequence. Denote by $a^{\langle k \rangle}$ the k-th power of a, which is defined

1991 Mathematics Subject Classification: 20N15, 16D10, 16D40
Keywords: free n-module, canonical presentation

by:

$$a^{\langle 0\rangle} = a \quad \text{and} \quad a^{\langle k\rangle} = [a^{\langle k-1\rangle}, \overset{(n-1)}{a}]_+, \quad k \in \mathbb{Z}$$

In particular, $a^{\langle -1\rangle} = \overline{a}$, where $\overline{a}$ denotes the querelement of a.

Throughout this paper R denotes an associative ring with unity $1 \neq 0$.

Definition 1.1. We call *left R-n-module* a commutative n-group $(M, [\,]_+)$ together with an external operation $\mu\colon R \times M \to M$ which satisfies the axioms:

A1) $\mu(r, [x_1^n]_+) = \big[\mu(r, x_1), \ldots, \mu(r, x_n)\big]_+$

A2) $\mu\big((r_1 + \cdots + r_n), x\big) = \big[\mu(r_1, x), \ldots, \mu(r_n, x)\big]_+$

A3) $\mu(r \cdot r', x) = \mu\big(r, \mu(r', x)\big)$

A4) $\mu(1, x) = x$

for all $x, x_1, \ldots, x_n \in M$ and all $r, r', r_1, \ldots, r_n \in R$.

We describe a *right R-n-module* by replacing in the above definition axiom A3) by A3') $\mu(r \cdot r', x) = \mu\big(r', \mu(r, x)\big)$. As in the binary case, the theory of right n-modules can be deduced from the theory of left n-modules and conversely. For this reason, we shall deal in the sequel with left n-modules, and by R-n-modules we shall always understand left R-n-modules.

Since we are dealing with left n-modules, denote the element $\mu(r, x)$ by rx. As immediate consequences of the axioms, note:

$$(r_1{+}r_2)x = [r_1x, r_2x, \overset{(n-2)}{0x}]_+, \qquad (-r)x = [0x, 0x, \overset{(n-3)}{rx}, r\overline{x}]_+,$$

$$\overline{rx} = r\overline{x}, \qquad \overline{x} = (-n{+}2)x = \big((-1){+}\cdots{+}(-1)\big)x.$$

The empty n-group may be regarded as an R-n-module for any ring R. If M is a non-empty R-n-module, then it necessarily has at least one neutral element; indeed, for every $x \in M$, the element $0x$ is a neuter in $(M, [\,]_+)$ (or an idempotent, since the two notions coincide in commutative n-groups). Note that $0x^{\langle k\rangle} = 0x$, $\forall x \in M$, $\forall k \in \mathbb{Z}$ (in particular $0x = 0\overline{x}$).

n-Submodules, congruences and homomorphisms are defined in the obvious way. If S is a non-empty n-submodule of an R-n-module M, then the relation ρ_S defined by $x\rho_S y \Leftrightarrow \exists s_2^n \in S : y = [x, s_2^n]_+$ is a congruence on M. This correspondence is not a bijection, still it allows us to define the factor module $M/S = M/\rho_S$.

The set of all neuters of the n-group $(M, [\,]_+)$ is denoted by $\mathcal{N}_M$ (or simply by $\mathcal{N}$) and the set of all neuters of the form $0x$, for some $x \in M$, is denoted by $\mathcal{N}_{0M}$ (or sometimes just $\mathcal{N}_0$). $\mathcal{N}_0$ is an n-submodule of $\mathcal{N}$ and they are both n-submodules of M. The elements of $\mathcal{N}_0$ are characterized by the following: $e \in \mathcal{N}_0 \Leftrightarrow re = e, \forall r \in R$. The elements of $\mathcal{N}_0$ will be called *zero-idempotents*; in particular, if $\mathcal{N}_0$ consists of exactly one element, then this element is called a *zero* of the n-module and it is denoted by 0.

If $f \colon M_1 \to M_2$ is a homomorphism of R-n-modules, then:

1) $f(\mathcal{N}_1) \subseteq \mathcal{N}_2$ and $f(\mathcal{N}_{01}) \subseteq \mathcal{N}_{02}$;

2) $f(\overline{x}) = \overline{f(x)}, \forall x \in M_1$;

3) the set $\operatorname{Ker} f = \{x \in M_1 \mid f(x) \in \mathcal{N}_{02}\}$ is an n-submodule of M_1 and $\mathcal{N}_{01} \subseteq \operatorname{Ker} f$.

2. The canonical presentation

2.1. We have introduced in [4] a class of n-submodules of an R-n-module which will play an important role in the study of n-modules. Let M be an R-n-module. For each $e \in \mathcal{N}_0$, the set

$$M_e = \{x \in M \mid 0x = e\}$$

is an n-submodule with zero (the element e) of M. The n-submodules M_e are all isomorphic and they form a partition of M. Note that $M/\mathcal{N}_0 \simeq M_e$. In fact, the whole structure of an R-n-module is determined by: the structure of an R-n-module with zero (M_e) and the structure of an idempotent commutative n-group ($\mathcal{N}_0$).

Indeed, if we start from an R-n-module $(B, [\,], \mu)$ with zero 0 and an idempotent commutative n-group $(A, [\,]_\circ)$, we can build an R-n-module M (unique up to isomorphism) such that $M_e \simeq B, \forall e \in \mathcal{N}_{0M}$ and $\mathcal{N}_{0M} \simeq A$, as follows:

- the set M is defined as the disjoint union, indexed by A, of copies of the set B: $M = \overset{\circ}{\bigcup\limits_{e\in A}} B_e$; denote by (x, e) the elements of B_e;
- the external operation $\nu\colon R \times M \to M$ is defined by
$$\nu\big(r, (x, e)\big) = \big(\mu(r, x), e\big)\,;$$
- n-ary addition is defined by
$$\big[(x_1, e_1), \ldots, (x_n, e_n)\big]_+ = \big([x_1^n], [e_1^n]_\circ\big).$$

A straightforward computation shows that $(M, [\,]_+, \nu)$ is an R-n-module such that

$$\mathcal{N}_{0M} = \{(0, e) \mid e \in A\} \simeq A \text{ and } M_{(0,e)} = \{(x, e) \mid x \in B\} \simeq B,$$

for each $(0, e) \in \mathcal{N}_{0M}$. Moreover, given an R-n-module T and performing the above construction by using some T_e instead of B and $\mathcal{N}_{0T}$ instead of A one obtains an R-n-module M which is isomorphic to T. A very natural isomorphism to consider is

$$\varphi\colon T \to M, \quad \varphi(x) = \big([x, \overset{(n-2)}{0x}, e]_+, 0x\big).$$

This shows that an R-n-module M is completely described by its largest n-submodule(s) with zero M_e and by $\mathcal{N}_{0M}$. This way of describing an R-n-module will be called *canonical presentation.* We have used disjoint union in order to construct an R-n-module with a given canonical presentation, because this was the natural way to make the connections with the M_e's and with $\mathcal{N}_0$. Yet, for practical reasons, it is simpler to consider the R-n-module being described as the Cartesian product $B \times A$, together with the operations defined above. Note that the map $p_1\colon B \times A \to B$, $p_1\big((x, e)\big) = x$ is a homomorphism of R-n-modules, and the map $p_2\colon B \times A \to A$, $p_2\big((x, e)\big) = e$ is a homomorphism of n-groups.

2.2. The canonical presentation of an R-n-module will prove its usefulness in the study of n-submodules and in the study of homomorphisms. Indeed, let M be an R-n-module with the canonical presentation $(B, [\,], \mu)$ and $(A, [\,]_\circ)$, as above. Then any n-submodule of M has a canonical presentation of the form $(B', [], \mu)$ and $(A', []_\circ)$, where B' is an n-submodule of B and A' is an n-subgroup of A.

Now let $f\colon M_1 \to M_2$ be a homomorphism of R-n-modules and take an arbitrary zero-idempotent $e \in \mathcal{N}_{01}$. Then $\varphi\colon \mathcal{N}_{01} \to \mathcal{N}_{02}$, $\varphi(x) = f(x)$ and $\psi\colon M_{1e} \to M_{2f(e)}$, $\psi(x) = f(x)$ are both homomorphisms. Moreover, the converse also holds, namely: if $\varphi\colon A_1 \to A_2$ is a homomorphism of n-groups and $\psi\colon B_1 \to B_2$ is a homomorphism of R-n-modules, then the map $f\colon M_1 \to M_2$ defined by

$$f\left((x,e)\right) = (\psi(x), \varphi(e))$$

is a homomorphism of R-n-modules (where M_1 and M_2 have the canonical presentations B_1, A_1 and B_2, A_2 respectively).

Injective and surjective homomorphisms can be also characterized in terms of the data of the canonical presentation.

Proposition 2.3. *Let $f\colon M_1 \to M_2$ be a homomorphism of R-n-modules. Then*

1) *f is injective iff* $\operatorname{Ker} f = \mathcal{N}_{01}$ *and the restriction $f|_{\mathcal{N}_{01}}$ is injective;*
2) *f is surjective iff for each $e' \in \mathcal{N}_{02}$ there exists $e \in \mathcal{N}_{01}$ such that $M_{2e'} = f(M_{1e})$.*

Proof. 1) Suppose f is injective and $x \in \operatorname{Ker} f$, i.e. $f(x) \in \mathcal{N}_{02}$. Then $f(x) = 0f(x) = f(0x)$, which implies $x = 0x$ and hence $x \in \mathcal{N}_{01}$.

Conversely, if $\operatorname{Ker} f = \mathcal{N}_{01}$ and the restriction $f|_{\mathcal{N}_{01}}$ is injective, let $f(x_1) = f(x_2)$. Then, for an arbitrary $e \in \mathcal{N}_{01}$, we have

$$f\big([x_1, \overset{(n-3)}{x_2}, \overline{x_2}, e]_+\big) = f(e) \in \mathcal{N}_{02},$$

i.e. $[x_1, \overset{(n-3)}{x_2}, \overline{x_2}, e]_+ \in \operatorname{Ker} f = \mathcal{N}_{01}$. Since $f|_{\mathcal{N}_{01}}$ is injective, it follows that $[x_1, \overset{(n-3)}{x_2}, \overline{x_2}, e]_+ = e$, hence $x_1 = x_2$.

2) Suppose f is surjective and $e' \in \mathcal{N}_{02}$. Then there exists $x \in M_1$ such that $e' = f(x)$; but $e' = 0e' = 0f(x) = f(0x) \in f(\mathcal{N}_{01})$. Denote $0x$ by $e \in \mathcal{N}_{01}$ and let $y \in M_{2e'}$ (this means $0y = e'$). Now there exists $u \in \mathcal{N}_{01}$ and $z \in M_{1u}$ such that $y = f(z)$. The element $[z, \overset{(n-2)}{u}, e]_+$ belongs to M_{1e} and $f\big([z, \overset{(n-2)}{u}, e]_+\big) = f(z) = y$. Thus, we have proved that for each $e' \in \mathcal{N}_{02}$ there exists $e \in \mathcal{N}_{01}$ such that $M_{2e'} \subseteq f(M_{1e})$; the other inclusion is obvious. The converse follows immediately from the fact that the n-submodules $M_{2e'}$ form a partition of M_2. □

3. Free n-modules with zero

R-n-modules with zero can be regarded as universal algebras having as domain of operations: an n-ary operation, a nullary operation and a family of unary operations, indexed by R, all of which satisfy the axioms A1)–A4). The class of R-n-modules with zero is a variety — it is closed under taking homomorphic images, subalgebras and direct products. This ensures the existence of free R-n-modules with zero. In this section we will provide a construction, very similar to the binary case, of the free R-n-module with zero having an arbitrary free generating set X.

Let A be an R-n-module with zero. The elements $a_1, \ldots, a_k \in A$, where $k \equiv t(\mathrm{mod} n{-}1)$, are called *linearly independent* if

$$[r_1a_1, \ldots, r_ka_k, \overset{(n-t)}{0}]_+ = 0 \quad \text{implies} \quad r_1 = \ldots = r_k = 0$$

and *linearly dependent* otherwise. A subset X of A is *linearly independent* if any finite subset of X is linearly independent. X is a *basis* of A if X is not empty, if X generates A, and if X is linearly independent. It is easy to prove that if X is a basis of A, then in particular $A \neq \{0\}$ if $R \neq \{0\}$ and every element of A has a unique expression as a linear combination of elements of X.

Proposition 3.1. *An R-n-module A with zero, which has a basis X, is free on X in the variety of R-n-modules with zero.*

Proof. Let T be an R-n-module with zero and a mapping $\alpha\colon X \to T$. Every element $a \in A$ has a unique expression of the form:

$$a = [r_1x_1, \ldots, r_kx_k, \overset{(n-t)}{0_A}]_+$$

where $k \equiv t(\mathrm{mod}\, n{-}1)$ and $r_1, \ldots, r_k \in R$, $x_1, \ldots, x_k \in X$.

Define $\widetilde{\alpha}\colon A \to T$ by $\widetilde{\alpha}(a) = [r_1\alpha(x_1), \ldots, r_k\alpha(x_k), \overset{(n-t)}{0_T}]_+$; a simple computation shows that $\widetilde{\alpha}$ is a homomorphism of R-n-modules and $\widetilde{\alpha} \circ i = \alpha$. Moreover, $\widetilde{\alpha}$ is the unique homomorphism with this property. □

Corollary 3.2. *Two R-n-modules with zero, having bases whose cardinalities are equal, are isomorphic.*

For this reason, we denote the R-n-module with zero free on X by

$F_0(X)$.

Let $X \neq \emptyset$ be an arbitrary set and a mapping $f\colon X \to R$. As usual, define

$$\operatorname{supp} f = \{x \in X \mid f(x) \neq 0\}$$

and

$$R^{(X)} = \{f \in R^X \mid |\operatorname{supp} f| < \infty\}.$$

We define a natural structure of R-n-module with zero on $R^{(X)}$ as follows:

$$[f_1, \ldots, f_n]_+(x) = f_1(x) + \cdots + f_n(x),\ (rf)(x) = r \cdot f(x).$$

The zero element is the function $o\colon X \to R,\ o(x) = 0,\ \forall x \in X$.

Proposition 3.3. *If $R \neq \{0\}$ is a ring and $X \neq \emptyset$ is an arbitrary set, then $R^{(X)}$ has a basis of the same cardinality as X.*

Proof. A basis of $R^{(X)}$ is the set $B = \{f_x \mid x \in X\}$, where $f_x\colon X \to R$ is defined by $f_x(y) = \begin{cases} 1, & y = x \\ 0, & y \neq x \end{cases}$.

One can easily check that B is linearly independent; furthermore, if $f \in R^{(X)}$ with $\operatorname{supp} f = \{x_1, \ldots, x_k\}$, where $k \equiv t (\mathrm{mod} n{-}1)$, then $f = [f(x_1) \cdot f_{x_1}, \ldots, f(x_k) \cdot f_{x_k}, \overset{(n-t)}{o}]_+$. □

Like in the binary case (see [5]), one can easily prove that if $F_0(X) \simeq F_0(Y)$ and X is infinite, then Y is infinite too and $|X| = |Y|$.

4. Free n-modules

The class of all R-n-modules is again a variety, so free R-n-modules exist. We will give in this final section a canonical presentation for the free R-n-module on an arbitrary set as well as a theorem concerning the number of zero-idempotents of a free R-n-module with a finite free generating set.

Note that, similar to the case of R-n-modules with zero, two free R-n-modules having free generating sets whose cardinalities are equal, are isomorphic.

Theorem 4.1. *Let $X \neq \emptyset$ be an arbitrary set and F be the R-n-module having the following canonical presentation:*

(a) *$F_0(X)$ as largest n-submodule with zero;*

(b) *the abelian n-group G with the presentation*

$$\left\langle X \mid [\overset{(n)}{x}]_+ = x,\ \forall x \in X \right\rangle$$

as idempotent commutative n-group.

Then the R-n-module F is free and X is its free generating set.

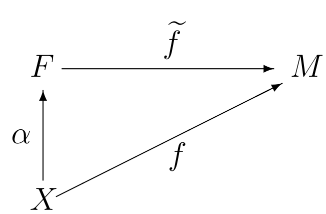
Proof. First, let us make some necessary remarks.
1) The n-group G described in *(b)* is the free idempotent abelian n-group with the free generating set X (it is easy to see that the class of idempotent abelian n-groups is a variety; as for the construction of free abelian n-groups, see the paper of F. M. Sioson [6]).
2) By 2.1, the elements of F have the form (y, g), where $y \in F_0(X)$ and $g \in G$. We shall identify each $x \in X$ with the pair $(x, x) \in F$; in other words, we define an "inclusion" $\alpha\colon X \to F$, by $\alpha(x) = (x, x)$.

Let M be an arbitrary R-n-module having the canonical presentation B, A, where B is an R-n-module with zero and A is an idempotent abelian n-group, as in 2.1. This means that we will describe the elements of M as pairs $(b, a) \in B \times A$. Let now $f\colon X \to M$ be an arbitrary map. We will use f for defining two other maps u and v as:

$$u\colon X \to B, \quad u(x) = p_1\left(f(x)\right) \tag{1}$$

$$v\colon X \to A, \quad v(x) = p_2\left(f(x)\right) \tag{2}$$

Since $F_0(X)$ is the free R-n-module with zero on X and B is an R-n-module with zero, it follows that there exists a unique homomorphism $\widetilde{u}\colon F_0(X) \to B$ such that $\widetilde{u}(x) = u(x)$, $\forall x \in X$. By using a similar argument, it follows that there exists a unique homomorphism of n-groups $\tilde{v}\colon G \to A$ such that $\widetilde{v}(x) = v(x)$, $\forall x \in X$. We are now able to define the homomorphism $\widetilde{f}$ which makes the following diagram commutative:



namely, for all $(y, g) \in F$, put $\widetilde{f}((y, g)) = (\widetilde{u}(y), \widetilde{v}(g))$. We have seen in 2.2 that a map defined in the above way is a homomorphism of R-n-modules. Further, for all $x \in X$ we have

$$(\widetilde{f} \circ \alpha)(x) = \widetilde{f}\big((x, x)\big) = \big(p_1\big(f(x)\big), p_2\big(f(x)\big)\big) = f(x)$$

which shows that $\widetilde{f} \circ \alpha = f$. The uniqueness of $\widetilde{f}$ follows from the uniqueness of $\widetilde{u}$ and $\widetilde{v}$ and from 2.2. □

Corollary 4.2. *Let X, Y be two non-empty sets. If $F(X) \simeq F(Y)$ and X is infinite, then Y is infinite too and $|X| = |Y|$.*

Proof. It follows immediately from the preceding theorem and from the similar result for free R-n-modules with zero. □

Lemma 4.3. *Let n be an integer, $n \geqslant 3$, X a set with $|X| = k$, $k \geqslant 1$ and $F(X)$ the R-n-module free on X. Then $\mathcal{N}_{0F(X)}$ has $(n-1)^{k-1}$ elements.*

Proof. Indeed, $\mathcal{N}_0$ is equal to

$$\{[\overset{(t_1)}{0x_1}, \overset{(t_2)}{0x_2}, \ldots, \overset{(t_k)}{0x_k}]_+ \mid 0 \leqslant t_i \leqslant n-2,\ t_1 + \cdots + t_k \equiv 1 (\mathrm{mod} n-1)\}$$

or, equivalently, $\mathcal{N}_0 \simeq G$, where G is the idempotent abelian n-group described in Theorem 4.1. Every element of $\mathcal{N}_0$ can be described by a uniquely determined function $f\colon \{1, \ldots, k-1\} \to \{0, 1, \ldots, n-2\}$ as follows:

$$e = [\overset{(f(1))}{0x_1}, \ldots, \overset{(f(k-1))}{0x_{k-1}}, \overset{(n-r)}{0x_k}]_+$$

where $f(1) + \cdots + f(k-1) = t(n-1) + r$, $2 \leqslant r \leqslant n$. This correspondence between elements of $\mathcal{N}_0$ and such functions is obviously a bijection and so $|\mathcal{N}_0| = (n-1)^{k-1}$. □

Corollary 4.4. *Let n be an integer, $n \geqslant 3$ and X, Y two non-empty sets. If $F(X) \simeq F(Y)$ and X is finite, then Y is finite too and $|X| = |Y|$.*

Proof. It follows from 2.2, Theorem 4.1 and the preceding lemma. □

The following theorem is a direct consequence of the preceding results in this section.

Theorem 4.5. *Let n be an integer, $n \geqslant 3$, and let X, Y be two non-empty sets. Then $F(X) \simeq F(Y)$ iff $|X| = |Y|$.*

Acknowledgements. This paper was written while the author was a visitor at Université Paris VII, in 1999. Thanks go to the members of the "Equipe des Groupes Finis" for their hospitality and support. The stay was supported by a scholarship from the Noesis Foundation, which is gratefully acknowledged.

References

[1] **N. Celakoski**, *On n-modules*, Godisen Zb. Elektro–Mas. Fak. Univ. Skopje **3** (1969), 15 – 26.

[2] **P. M. Cohn**, *Universal algebra*, Second edition, Mathematics and its Applications **6**, D. Reidel Publishing Co., Dordrecht – Boston, Mass. , 1981.

[3] **W. Dörnte**, *Untersuchungen über einen verallgemeinerten Gruppenbegriff*, Math. Z. **29** (1928), 1 – 19.

[4] **L. Iancu**, *Redefining n-modules*, Bul. Şt. Univ. Baia Mare, Ser. B, Mat.–Inf. **14** (1998)

[5] **I. Purdea**, *Tratat de algebră modernă*, Vol.II, (Romanian) (*Treatise on modern algebra. Vol.II*) Ed. Academiei RSR, Bucharest, 1982.

[6] **F. M. Sioson**, *Free Abelian m-Groups, I, II, III*, Proc. Japan Acad. **43** (1967), 876 – 888.

Received January 27, 1999

North University of Baia Mare
Victoriei 7
RO–4800 Baia Mare
Romania
e-mail: liancu@ubm.ro

current address:
Institut Girard Desargues
Bat. 101, Université Lyon 1
43 Bd du 11 Novembre 1918
F-69622 Villeurbanne Cedex
France
e-mail: iancu@desargues.univ-lyon1.fr