CODES OVER RINGS AND MODULES

ÁNGEL DEL RÍO

1. Introduction

Two relevant results of MacWilliams are the Extension Property and the MacWilliams Identities for linear codes. The first one describes the isomorphisms preserving the Hamming weight between linear codes and the second one relates the weight distribution of a linear code and its dual. In this note we revise some recent results of several authors (mostly of J. A. Wood) which describes when the Extension Property and the MacWilliams Identities hold in the more general settings of linear codes over modules. We basically follow the approach of [Woo09].

We start recalling the statements of the Extension Property and the MacWilliams Identities. Let F be a field and let n be a positive number. A *monomial transformation* of F^n is a map $T : F^n \to F^n$ of the form

$$T(a_1, \dots, a_n) = (u_1 a_{\sigma(1)}, \dots, u_n a_{\sigma(n)}) \quad (a_1, \dots, a_n) \in F^n,$$

for some $\sigma \in S_n$ and $u_1, \dots, u_n \in \mathcal{U}(F) = F \setminus \{0\}$. Observe that if T is a monomial transformation of F^n then T is an isomorphism of M^n preserving the Hamming weight (i.e. $w(f(x)) = w(x)$ for every $x \in F^n$). The Extension Property states that monomial transformations are the only maps satisfying these conditions, in a very strong way:

1.1. Theorem [Extension Property] [Mac61, Mac62] *Let F be finite field, let C_1 and C_2 be linear codes of length n over the alphabet F and let $f : C_1 \to C_2$ be an isomorphism of vector spaces preserving the Hamming weight. Then f extends to an α-monomial transformation of F^n.*

The *weight enumerator* of a linear code C of length n is the following polynomial in two variables:

$$W_C(X, Y) = \sum_{c \in C} X^{n-w(c)} Y^{w(c)} = \sum_{i=0}^{n} A_{C,i} X^{n-i} Y^j,$$

where $A_{C,i}$ denotes the number of codewords of C of weight i.

1.2. Theorem [MacWilliams Identities] [Mac63, Mac62] *Let F be a finite field of cardinality q and let C be a linear code over the alphabet F. Then*

$$W_{C^\perp}(X, Y) = \frac{1}{|C|} W_C(X + (q-1)Y, X - Y). \tag{1.1}$$

The vector $A_C = (A_{C,i})_{i=0,1,\dots,n}$ is call the *weight distribution* of C. As this vector determines the coefficients of $W_C(X, Y)$, the MacWilliams identities gives the weight distribution of a code in terms of the weight distribution of its dual (and vice versa). More precisely, comparing the coefficients in the two sides of the equation (1.1) we have

$$A_{C^\perp,i} = \frac{1}{|C|} \sum_{j=0}^{n} A_{C,j} \sum_{l=0}^{i} \binom{n-j}{i-l} \binom{j}{l} (q-1)^{i-l} (-1)^l.$$

2. Rings and modules

In this section we introduce the basic notions on rings and modules.

A *ring* is a set R together with two operations, a sum and a product,

$$\begin{array}{ccccc} R \times R & \stackrel{+}{\to} & R & \qquad R \times R & \stackrel{\cdot}{\to} & R \\ (r, s) & \mapsto & r + s & \qquad (r, s) & \mapsto & rs \end{array}$$

such that the sum makes $(R, +)$ an abelian group (with zero denoted 0 and opposite of $r \in R$ denoted $-r$), the multiplication is associative and has an identity 1, (i.e. $1r = r1 = r$ for every $r \in R$) and the product distributes the sum (i.e. $r(s + t) = rs + rt$ and $(r + s)t = rt + st$ for every $r, s, t \in$). If the product is commutative then we say that R is a *commutative ring*. The elements of R which are invertible with

Partially supported by Ministerio de Economía y Competitividad project MTM2012-35240 and Fondos FEDER and Fundación Séneca of Murcia 19880/GERM/15.

respect to the product are called units of R and form a group, denoted $\mathcal{U}(R)$. A *division ring* is a ring with $\mathcal{U}(R) = R \setminus \{0\}$; a field is a commutative division ring.

Let R be a ring. A *subring* of R is a subset which is a ring with the restriction of the sum and product of R. A *left ideal* of R is a subgroup I of $(R, +)$ satisfying $rx \in I$ for every $r \in R$ and $x \in I$. *Right ideals* are defined similarly. An *ideal* is a left ideal which is also a right ideal.

Modules are simply vector spaces over rings (rather than over fields). More precisely, a *right R-module* (or *right module* over R) is an additive abelian group M together with a product

$$\begin{array}{rcl} M \times R & \to & M \\ (m, r) & \mapsto & mr \end{array}$$

satisfying the following conditions for every $r, s \in R$ and $m, n \in M$:

$$(m + n)r = mr + nr, \quad m(r + s) = mr + ms, \quad m(rs) = (mr)s \quad \text{and} \quad m1 = m.$$

Left modules are defined similarly. If R is commutative then every right R-module is also a left module with multiplication $rm = mr$ and hence we simply will call them modules. However if R is non-commutative then right and left R-modules can be very different.

Let M be a right R-module. A *submodule* of M is an additive subgroup N of M satisfying $nr \in N$ for every $n \in N$ and $r \in R$.

If R and S are two rings then an (R, S)-bimodule is a left R-module which is also a right S-module and satisfies the following equality for every $r \in R$, $s \in S$ and $m \in M$.

$$r(ms) = (rm)s.$$

A *ring homomorphism* is a map $f : R \to S$ between rings satisfying

$$f(r + s) = f(r) + f(s), \quad f(rs) = f(r)f(s) \quad \text{and} \quad f(1) = 1.$$

A *module homomorphism* (of right R-modules) is a map $f : M \to N$ between modules satisfying the following condition for every $r \in R, m, n \in M$:

$$f(m + n) = f(m) + f(n), \quad f(mr) = f(m)r.$$

Homomorphisms of left R-modules are defined similarly. An *isomorphism* of rings (resp. modules) is a bijective ring (module) homomorphism. Two rings (resp. modules) are *isomorphic* if there is an isomorphism from one to the other. An *endomorphism* of a module M is a homomorphism $M \to M$. An *automorphism* of M is a bijective endomorphism of M.

We consider homomorphisms of right modules as left operators and homomorphisms of left modules as right operators. More precisely, if $f : M \to N$ is a homomorphism of right (resp. left) R-modules then the image of $m \in M$ by f is denoted fm (resp. mf). If $g : N \to P$ is another homomorphism of right (resp. left) R-modules then the composition $g \circ f$ is denoted gf (resp. fg).

Often it is not relevant whether we use left of right R-modules and in this case we forget the convention of the previous paragraph and use the standard notation $f(m)$, for action of f on m.

2.1. Examples [Rings and modules]

1. The most classical examples of commutative rings are the ring of integers, denoted $\mathbb{Z}$, the fields of rationals, $\mathbb{Q}$, real numbers, $\mathbb{R}$, and complex numbers, $\mathbb{C}$.

   Modules over $\mathbb{Z}$ are simply abelian groups.
2. An important family of finite commutative rings is the one formed by the ring $\mathbb{Z}/n\mathbb{Z}$. Modules over $\mathbb{Z}/n\mathbb{Z}$ are abelian groups A satisfying $nA = 0$.

   This example can be generalized to quotient rings R/I with R any ring and I any ideal of R, formed by the equivalence classes $r + I = \{r + x : x \in I\}$ of the equivalent relation modulo I ($r \equiv s \mod I \Leftrightarrow r - s \in I$). The sum and product in R/I are defined in the natural way:

   $$(r + I) + (s + I) = (r + s) + I, \quad (r + I)(s + I) = rs + I.$$

   The map $r \mapsto r + I$ is a ring homomorphism $\pi_I : R \to R/I$.

   If M right R/I-module then it is also a right R-module with the product $mr = m(r + I)$. In that case $MI = 0$. Conversely, if M is a right R-module satisfying $MI = 0$ then M is also a right R/I-module with the product $m(r + I) = mr$. Therefore we can identify right R/I-modules with the right R-modules M satisfying $MI = 0$.
3. If M is right R-module and N is a submodule of M then the quotient additive group M/N is right R-module with the natural product:

   $$(m + N)r = mr + N, \quad (m \in M, r \in R).$$

   The map $K \mapsto K/N$ is a one-to-one correspondence, preserving inclusion, from the set of submodules of M containing N to the set of submodules of M/N.

4. If $\{R_i : i \in I\}$ is a family of rings then the direct product $\prod_{i\in I} R_i$ is a ring with the obvious sum and product.
5. A classical family of example of non-commutative rings encountered in linear algebra are the matrix rings $M_n(F)$, with F a field and n a positive integers. This example can be generalized to any ring in a straightforward way.

   The upper triangular matrices in $M_n(R)$ (i.e. the matrices having 0 below the diagonal) form a subring of $M_n(R)$.
6. Another linear algebra example of rings is the ring of endomorphisms of a vector space. This example can also be generalized to the ring of endomorphisms of a module where the sum and product is given in the natural way:
$$(f+g)m = fm + gm, \quad (fg)m = f(gm).$$
   If M and N are right R-modules then the set of homomorphism from M to N is denoted $\mathrm{Hom}_R(M,N)$ (or $\mathrm{Hom}(M_R, N_R)$, or $\mathrm{Hom}(M_R, N)$ or $\mathrm{Hom}(M, N_R)$, if we want to emphasize that they are right R-modules). It is an abelian group with the following sum:
$$(f+g)m = fm + gm, \quad f, g \in \mathrm{Hom}(M_R, N_R).$$
   The ring of endomorphisms of M is denoted $\mathrm{End}_R(M)$ (or $\mathrm{End}(M_R)$). Then $\mathrm{Hom}(M_R, N_R)$ is an $(\mathrm{End}(N_R), \mathrm{End}(M_R))$-bimodule with composition used as product.

   In case M and N are left modules, $\mathrm{Hom}({}_RM, {}_RN)$ is a $(\mathrm{End}({}_RM), \mathrm{End}({}_RN))$-bimodule with reverse composition used as product.
7. Let R and S be rings, let ${}_SM_R$ be an (S,R)-bimodule and N_R a right R-module. Then $\mathrm{Hom}(M_R, N_R)$ is a right S-module with multiplication given by $(fs)(m) = f(sm)$. Similarly, if M_R is a right R-module and ${}_SN_R$ is an (S,R)-bimodule then $\mathrm{Hom}(M_R, N_R)$ is a left S-module with multiplication given by $(sf)m = s(fm)$.

   Similar structures are obtained using homomorphisms of left R-modules.
8. Let R be a ring. Then R is a right and left R-module in the obvious way. We denote the left R-module as ${}_RR$ and the right R-module as R_R.

   Let M be a right R-module. If $m \in M$ then the map $\lambda_m : R \to M$ given by $\lambda_m(r) = mr$ is an isomorphism of right R-modules $M \to \mathrm{Hom}(R_R, M_R)$ ($(\lambda_m r)s = \lambda_m(rs) = mrs = \lambda_{mr}(s)$). In case $M = R_R$ this isomorphisms is a ring isomorphism $R \cong \mathrm{End}(R_R)$.
9. Let M be a module and let $\{N_i : i \in I\}$ be a family of submodules of M. Then the intersection $\cap_{i\in I} N_i$ is a greatest submodule of M contained in all the M_i. The smallest submodule containing all the M_i is the sum
$$\sum_{i\in I} N_i = \left\{ \sum_{i\in I} n_i, n_i \in N_i, \text{ for every } i \text{ and } n_i = 0 \text{ for all but finitely many } i \right\}.$$
   We say that $\{N_i : i \in I\}$ is *independent* if $N_i \cap \sum_{j\neq i} N_j = \{0\}$ for every $i \in I$. In this case the sum $\sum_{i=1}^k N_i$ is usually denoted $\oplus_{i\in I} N_i$ (or $N_1 \oplus \cdots \oplus N_k$ if $I = \{1, \ldots, k\}$) and called the (internal) *direct sum* of $\{N_i : i \in I\}$.

   If $\{M_i : i \in I\}$ is a family of modules then the cartesian product $\prod_{i\in I} M_i$ is a module, with the natural sum and product. The subset of $\prod_{i\in I} M_i$ formed by the tuples having only finitely many non-zero entries is a submodule called the (external) *direct sum* of $\{M_i : i \in I\}$ (denoted $\oplus_{i\in I} M_i$ or $M_1 \oplus \cdots \oplus M_k$ in case $I = \{1, \ldots, k\}$). The elements of $\oplus_{i\in I} M_i$ having 0 at all the coordinates different from the i-th form a submodule N_i of M, isomorphic to M_i and $\oplus_{i\in I} M_i = \oplus_{i\in I} N_i$. In this way we may identify external and internal direct sums.

   If $M_i = M$ for every i then the direct product $\prod_{i\in I} M_i$ is denoted M^I and the direct sum $\oplus_{i\in I} M_i$ is denoted $M^{(I)}$, or simply M^k if I is a finite set with k elements.
10. Let $f : R \to S$ be a ring homomorphism. Then $\mathrm{Im}\, f = \{f(r) : r \in R\}$ is a subring of S and $\ker f = \{r \in R : f(r) = 0\}$ is an ideal of R. Moreover, f is injective if and only if $\ker f = \{0\}$. If M is a right S-module then M is also a right R-module with the multiplication $mr = mf(r)$. This R-module is said to be obtained by *restriction of scalars*.
11. If $f : M \to N$ is a module homomorphism then $\mathrm{Im}\, f$ is a submodule of N and $\ker f$ is a submodule of M. Moreover f is injective if and only if $\ker f = \{0\}$. Furthermore, if f is bijective then f^{-1} is also an homomorphism.

Let $\{M_i : i \in I\}$ be a family of modules. Then for every $i \in I$ there are homomorphisms $\mu_i : M_i \to \oplus_{i\in I} M_i$ and $\pi_i : \prod_{i\in I} M_i \to M_i$, where $\pi_i((x_i)_{i\in I}) = x_i$ and $\mu_i(x)$ is the element of M having x at the i-th coordinate and 0 at the other coordinates.

If $f : \oplus_{i\in I} M_i \to N$ is a homomorphism then $f\mu_i : M_i \to N$ is a homomorphism. Conversely, if $f_i : M_i \to N$ is a homomorphism for every $i \in I$ then the map $(m_i)_{i\in I} \mapsto \sum_{i\in I} f_i(m_i)$ is the unique

homomorphism $f : \oplus_{i\in I} M_i \to N$ such that $f\mu_i = f_i$ for every i. This gives an isomorphism

$$\mathrm{Hom}(\oplus_{i\in I} M_i, N) \cong \prod_{i\in I} \mathrm{Hom}(M_i, N). \tag{2.2}$$

If $f : N \to \prod_{i\in I} M_i$ is a homomorphism then each $\pi_i f : N \to M_i$ is a homomorphism. Moreover, if $f_i : N \to M_i$ is a homomorphism for every $i \in I$, then the map $n \mapsto (f_i(n))_{i\in I}$ is the unique homomorphism $f : N \to \prod_{i\in I} M_i$ such that $\pi_i f = f_i$ for every i. This gives an isomorphism

$$\mathrm{Hom}\left(N, \prod_{i\in I} M_i\right) \cong \prod_{i\in I} \mathrm{Hom}(N, M_i).$$

Suppose now that $M = \oplus_{i=1}^m M_i$ and $N = \oplus_{j=1}^n N_j$. Then we have

$$\mathrm{Hom}_R(\oplus_{i=1}^m M_i, \oplus_{j=1}^n N_j) \cong \oplus_{i=1}^m \oplus_{j=1}^n \mathrm{Hom}_R(M_i, N_j).$$

We can display the elements of $\oplus_{i=1}^m \oplus_{j=1}^n \mathrm{Hom}_R(M_i, N_j)$ in matrix form, so that for right modules, we can identify

$$\mathrm{Hom}_R(\oplus_{i=1}^m M_i, \oplus_{j=1}^n N_j) \cong \begin{pmatrix} \mathrm{Hom}_R(M_1, N_1) & \mathrm{Hom}_R(M_2, N_1) & \dots & \mathrm{Hom}_R(M_m, N_1) \\ \mathrm{Hom}_R(M_1, N_2) & \mathrm{Hom}_R(M_2, N_2) & \dots & \mathrm{Hom}_R(M_m, N_l) \\ \dots & \dots & \dots & \dots \\ \mathrm{Hom}_R(M_1, N_n) & \mathrm{Hom}_R(M_2, N_n) & \dots & \mathrm{Hom}_R(M_m, N_n) \end{pmatrix}. \tag{2.3}$$

If moreover we display the elements $\oplus_{i=1}^k M_i$ and $\oplus_{j=1}^l N_j$ as column vectors we can interpret the action of a matrix on a column vector using the standard matrix arithmetics:

$$\begin{pmatrix} f_{1,1} & f_{2,1} & \dots & f_{m,1} \\ f_{1,2} & f_{2,2} & \dots & f_{m,2} \\ \dots & \dots & \dots & \dots \\ f_{1,n} & f_{2,n} & \dots & f_{m,n} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^n f_{i,1} x_i \\ \sum_{i=1}^n f_{i,2} x_i \\ \vdots \\ \sum_{i=1}^m f_{i,n} m_i \end{pmatrix}.$$

In particular we can identify

$$\mathrm{End}_R(\oplus_{i=1}^m M_i) \cong \begin{pmatrix} \mathrm{Hom}_R(M_1, M_1) & \mathrm{Hom}_R(M_2, M_1) & \dots & \mathrm{Hom}_R(M_m, M_1) \\ \mathrm{Hom}_R(M_1, M_2) & \mathrm{Hom}_R(M_2, M_2) & \dots & \mathrm{Hom}_R(M_k, M_l) \\ \dots & \dots & \dots & \dots \\ \mathrm{Hom}_R(M_1, M_m) & \mathrm{Hom}_R(M_2, M_m) & \dots & \mathrm{Hom}_R(M_m, M_m) \end{pmatrix} \tag{2.4}$$

and

$$\mathrm{End}_R(M^m) \cong M_m(\mathrm{End}_R(M)) \tag{2.5}$$

For left R-modules we use the transposes of the previous matrices.

Let M be a module and let X be a subset of M. The submodule of M *generated by* X is the smallest submodule of M containing X. We will denote this submodule as XR for right modules, and RX for left modules. The submodule generated by X can be described both as the intersection of all submodules of M containing X and as the set of R-linear combinations of elements of X. We say that M is generated by X if it coincides with the submodule generated by X. A module is said to be *finitely generated* if it is generated by a finite set and *cyclic* if it is generated by one element.

A module M is said to be free if it is of the form $R_R^{(I)}$ for some set I. If M is an arbitrary right R-module and I is a set $M^I \cong \mathrm{Hom}(R_R, M_R)^I \cong \mathrm{Hom}_R(R^{(I)}, M)$. This isomorphism maps $m = (m_i)$ to the homomorphism $\rho_m : R^{(I)} \to M$ mapping $(r_i)_{i\in I} \in R^{(I)}$ to $\sum_{i\in I} m_i r_i$. The image of ρ_m is $\sum_{i\in I} m_i R$, the submodule of M generated by the coordinates of M. If the coordinates of m generates M (for example $I = M$ and $m_i = i$ for every i) then ρ_m is surjective and hence M is isomorphic to an epimorphic image of $R^{(I)}$, by the First Isomorphism Theorem. This shows that every module is an epimorphic image of a free module. It also shows that a module is finitely generated if and only if it is a quotient of R^n for some positive integer n and it is cyclic if and only if it is a quotient of R.

3. Modules as alphabets

Let M be a module. We consider M as the alphabet to construct codes so that we only consider codes which are submodules of M^n for some positive integer n. More precisely a *linear code* of length n in the alphabet M is a submodule of M^n. The Hamming weight of an element $x \in M^n$ is the number $w(x)$ of non-zero entries of x. One specially relevant case is the one on which $M = R_R$ (or ${}_R R$).

A monomial transformation on M^n is a map $f : M^n \to M^n$ of the form

$$f(m_1, \dots, m_n) = (\alpha_1 m_{\sigma(1)}, \dots, \alpha_n m_{\sigma(n)}), \quad (m_1, \dots, m_n) \in M^n$$

for some $\sigma \in S_n$ and $\alpha_1, \ldots, \alpha_n \in \mathrm{Aut}(M_R)$.

We say that the alphabet M *satisfies the extension property* (EP for short) for length n if every isomorphism $f : C_1 \to C_2$ preserving the Hamming weight, with C_1 and C_2 linear codes of length n on the alphabet M, extends to a monomial transformation of M^n. We say that the alphabet M has the EP if it has the EP for every length.

In the remainder of the section we construct a module without the EP. For that we fix a finite field F with cardinality q and positive integers n and m. Let $R = \mathrm{End}_F(F^m)$ and $M = \mathrm{Hom}_F(F^n, F^m)$. Then M is a left R-module (see Examples 2.1.6). We will show that if $n > m$ then the alphabet M as right R-module does not have the EP.

We need some preparation. Suppose that $n \geq m$ and let $\left[\begin{array}{c} n \\ m \end{array} \right]_q$ denote the number of subspaces of F^n dimension m. We start proving

$$\left[\begin{array}{c} n \\ m \end{array} \right]_q = \begin{cases} 1, & \text{if } m = 0; \\ \prod_{i=0}^{m-1} \frac{q^{n-i}-1}{q^{m-i}-1}, & \text{if } m \neq 0. \end{cases}$$

Indeed, the case $m = 0$ is obvious. Suppose that $m \neq 0$ and let $\alpha_{n,m}$ denote the number of lists $(v_1, \ldots, v_m)$ formed by m linearly independent elements of F^n. To construct one of these lists we first select $v_1 \in F^n \setminus \{0\}$, then $v_2 \in F^n \setminus Fv_1$, $v_3 \in F^n \setminus Fv_1 + Fv_2$, and so on. Thus we have $q^n - 1$ options for v_1, $q^n - q$ options for v_2 and in general $q^n - q^{i-1}$ for v_i. This gives $\alpha_{n,m} = \prod_{i=0}^{m-1}(q^n - q^i)$. Two of these lists $(v_1, \ldots, v_n)$ and $(w_1, \ldots, w_n)$ generate the same subspace of F^n if and only if there is an invertible matrix $A = (a_{ij})_{1 \leq i,j \leq m}$ such that $w_i = \sum_{j=1}^{m} a_{ij} v_j$. Clearly the number of these invertible matrices is $\alpha_{m,m}$. Thus $(v_1, \ldots, v_m) \to \langle v_1, \ldots, v_m \rangle$ gives a surjective map from the set of list with m linearly independent elements of F^n to the set of m-dimensional subspaces of F^n, and the preimage of each subspace is a subset with $\alpha_{m,m}$ elements. Therefore

$$\left[\begin{array}{c} n \\ m \end{array} \right]_q = \frac{\alpha_{n,m}}{\alpha_{m,m}} = \prod_{i=0}^{m-1} \frac{q^n - q^i}{q^m - q^i} = \prod_{i=0}^{m-1} \frac{q^{n-i} - 1}{q^{m-i} - 1},$$

as desired.

We now prove the following recursion formula for $1 \leq m < n$:

$$\left[\begin{array}{c} n \\ m \end{array} \right]_q q^{\binom{m}{2}} = \left[\begin{array}{c} n-1 \\ m \end{array} \right]_q q^{\binom{m}{2}} + \left[\begin{array}{c} n-1 \\ m-1 \end{array} \right]_q q^{n-1+\binom{m-1}{2}} \quad (1 \leq m \leq n-1). \tag{3.6}$$

Indeed, using the well known formula $m - 1 + \binom{m-1}{2} = \binom{m-1}{1} + \binom{m-1}{2} = \binom{m}{2}$ we have

$$\begin{aligned} \left[\begin{array}{c} n-1 \\ m \end{array} \right]_q q^{\binom{m}{2}} \quad + \quad & \left[\begin{array}{c} n-1 \\ m-1 \end{array} \right]_q q^{n-1+\binom{m-1}{2}} \\ = \quad & \left(\prod_{i=0}^{m-1} \frac{q^{n-1-i}-1}{q^{m-i}-1} \right) q^{\binom{m}{2}} + \left(\prod_{i=0}^{m-2} \frac{q^{n-1-i}-1}{q^{m-i-1}-1} \right) q^{n-1+\binom{m-1}{2}} \\ = \quad & \frac{\prod_{i=0}^{m-2}(q^{n-1-i}-1)}{\prod_{i=0}^{m-1}(q^{m-i}-1)} \left((q^{n-m}-1) q^{\binom{m}{2}} + q^{n-1+\binom{m-1}{2}} (q^m - 1) \right) \\ = \quad & \frac{\prod_{i=0}^{m-2}(q^{n-1-i}-1)}{\prod_{i=0}^{m-1}(q^{m-i}-1)} \left(q^{n+\binom{m}{2}} - q^{\binom{m}{2}} \right) \\ = \quad & \frac{\prod_{i=0}^{m-1}(q^{n-1-i}-1)}{\prod_{i=0}^{m-1}(q^{m-i}-1)} q^{\binom{m}{2}} = \left[\begin{array}{c} n \\ m \end{array} \right]_q q^{\binom{m}{2}} \end{aligned}$$

3.1. Lemma [Cauchy Binomial Theorem] *For every positive integer n we have*

$$\prod_{i=0}^{n-1} (1 + q^i X) = \sum_{m=0}^{n} \left[\begin{array}{c} n \\ m \end{array} \right]_q q^{\binom{m}{2}} X^m.$$

Proof. We argue by induction on n with the case $n = 1$ been an obvious consequence of $\left[\begin{array}{c} 1 \\ 0 \end{array}\right]_q = \left[\begin{array}{c} 1 \\ 1 \end{array}\right]_q = 1$ and $\binom{0}{2} = \binom{1}{2} = 0$. For the induction step we use that $\left[\begin{array}{c} k \\ 0 \end{array}\right]_q = \left[\begin{array}{c} k \\ k \end{array}\right]_q = 1$ for every k and (3.6) as follows

$$\begin{aligned}
\prod_{i=0}^{n-1}(1+q^iX) &= \left(\sum_{m=0}^{n-1}\left[\begin{array}{c} n-1 \\ m \end{array}\right]_q q^{\binom{m}{2}}X^m\right)(1+q^{n-1}X) \\
&= \left[\begin{array}{c} n-1 \\ 0 \end{array}\right]_q q^{\binom{0}{2}}X^m + \sum_{m=1}^{n-1}\left(\left[\begin{array}{c} n-1 \\ m \end{array}\right]_q q^{\binom{m}{2}} + \left[\begin{array}{c} n-1 \\ m-1 \end{array}\right]_q q^{n-1+\binom{m-1}{2}}\right)X^m \\
&\quad + \left[\begin{array}{c} n-1 \\ n-1 \end{array}\right]_q q^{n-1+\binom{n-1}{2}} \\
&= \left[\begin{array}{c} n \\ 0 \end{array}\right]_q q^{\binom{0}{2}}X^m + \sum_{m=1}^{n-1}\left[\begin{array}{c} n \\ m \end{array}\right]_q q^{\binom{m}{2}}X^m + \left[\begin{array}{c} n \\ n \end{array}\right]_q q^{\binom{n}{2}} \\
&= \sum_{m=0}^{n}\left[\begin{array}{c} n \\ m \end{array}\right]_q q^{\binom{m}{2}}X^m.
\end{aligned}$$

□

Evaluating $X = 1$ and $X = -1$ in the formula of the Cauchy Binomial Theorem (Lemma 3.1) we obtain

$$\sum_{m=0}^{n}\left[\begin{array}{c} n \\ m \end{array}\right]_q q^{\binom{m}{2}} = 2\prod_{i=1}^{n-1}(1+q^i) \tag{3.7}$$

$$\sum_{m=0}^{n}(-1)^m\left[\begin{array}{c} n \\ m \end{array}\right]_q q^{\binom{m}{2}} = \begin{cases} 1, & \text{if } n = 0; \\ 0, & \text{if } n > 0. \end{cases} \tag{3.8}$$

3.2. Example [Wood] *Let F be a finite field, let $n > m > 0$ and consider the ring $R = \mathrm{End}_F(F^m)$ and the left R-module $M = \mathrm{Hom}_F(F^n, F^m)$. Then there is a positive integer N and two linear codes C_+ and C_- of M^N satisfying the following conditions:*

1. *one of the coordinates is 0 for all the codewords of C_+ but no coordinate is 0 for all the codewords of C_-.*
2. *There is an isomorphism $f : C_+ \to C_-$ preserving the Hamming weight.*

By 1, the isomorphism f does not extend to a monomial transformation of M^N and hence the alphabet does not satisfies the EP.

Proof. Let $V = F^n$ as an n-dimensional vector space over F. Let $S = \mathrm{End}_F(V)$. Then M is an (R, S)-bimodule (see Examples 2.1.6). For every subspace W of V let us fix $\lambda_W \in S$ with $\mathrm{Im}\,\lambda_W = W$. Let $N = \prod_{i=1}^{n-1}(1+q^i)$, $N_+ = \sum_{m=0, m \text{ even}}^{n}\left[\begin{array}{c} n \\ m \end{array}\right]_q q^{\binom{m}{2}}$ and $N_- = \sum_{m=0, m \text{ odd}}^{n}\left[\begin{array}{c} n \\ m \end{array}\right]_q q^{\binom{m}{2}}$. By (3.7), $2N = \sum_{m=0}^{n}\left[\begin{array}{c} n \\ m \end{array}\right]_q q^{\binom{m}{2}} = N_+ + N_-$ and by (3.8) $N_+ - N_- = 0$. Therefore $N = N_+ = N_-$. Let $\lambda : V \to V^{2N}$ be the map associating to each $v \in V$ the vector obtaining by putting $\binom{\dim W}{2}$ times the element $\lambda_W(v)$ for each subspace W of V. (Here we have preselected a certain order in the coordinates of V^{2N} so that we always use the same map λ_W in a given coordinate. The order chosen is not relevant but it should be fixed from the beginning. In that way the coordinates of V^{2N} are parametrized by the subspaces of V and each subspace of V of dimension k parametrizes $\binom{k}{2}$ different coordinates.) Let $\lambda_+ : V \to V^N$ be the composition of λ with the projection on the coordinates parametrized by subspaces with even dimension and $\lambda_- : V \to V^N$ be the composition of λ with the projection on the coordinates parametrized by subspaces with odd dimension. We now construct two homomorphisms of left R-modules $g_+, g_- : M \to M^N$ associating each $f \in M = \mathrm{Hom}_F(F^m, V)$ with the vector formed by the compositions $f\lambda_W$, with W of even dimension for g_+ and W of odd dimension for g_-.

We claim that $w(g_+(f)) = w(g_-(f))$. Indeed, each coordinate of $g_+(f)$ or $g_-(f)$ is of the form $f \circ \lambda_W$ and it is zero if and only if $W \subseteq \ker f$. Thus if we set

$$\delta(W) = \begin{cases} 0, & \text{if } W \subseteq \ker f; \\ 1 & \text{if } W \not\subseteq \ker f. \end{cases},$$

and $u = \dim \ker f$, then $u > 0$ because $n > m$ and

$$\begin{aligned} w(g_+(f)) - w(g_-(f)) &= \sum_{W \leq V} (-1)^{\dim W} q^{\binom{\dim W}{2}} \delta(W) \\ &= \sum_{W \leq V} (-1)^{\dim W} q^{\binom{\dim W}{2}} - \sum_{W \leq \ker f} (-1)^{\dim W} q^{\binom{\dim W}{2}} \\ &= \sum_{k=0}^{n} (-1)^k \begin{bmatrix} n \\ k \end{bmatrix}_q q^{\binom{k}{2}} - \sum_{k=0}^{u} (-1)^k \begin{bmatrix} u \\ k \end{bmatrix}_q q^{\binom{k}{2}} = 0 - 0 = 0 \end{aligned}$$

by (3.8). This proves the claim.

Moreover, if $f \neq 0$ then there $f\lambda_V \neq 0$ and hence either $g_+(f) \neq 0$ or $g_-(f) \neq 0$. Actually both are non-zero because they have the same Hamming weight. This shows that g_+ and g_- are injective and hence the map $g_+(f) \mapsto g_-(f)$ is a well defined homomorphism preserving the Hamming weight from $C_+ = \operatorname{Im} g_+$ to $C_- = \operatorname{Im} g_-$. One of the coordinates is zero for all the elements of C_+, namely the one corresponding to $W = 0$. However, no coordinate is zero for all the elements of C_-. Indeed, each coordinate of the codewords of C_- is parametrized by one non-zero subspace W of V (of odd dimension). If $w \in W \setminus \{0\}$ then there is $f \in M$ with $f(w) \neq 0$. Then the coordinate of $g_+(f)$ parametrized by W is $f \circ \lambda_W \neq 0$. This finishes the proof. □

4. Semisimple rings and modules

Let M be a module (whether it is left of right module it is irrelevant for the moment and only in case it is relevant the side we will mention it). If $M = \{0\}$ then we denote $M = 0$ and it has a unique submodule, namely M. Otherwise it has at least two different modules, namely M and 0. We say that M is *simple* if it has exactly two submodules. A module is said to be *semisimple* if it is a sum of simple submodules.

4.1. Lemma [The Schur's Lemma] *Let M and N be two simple modules. If $f : M \to N$ is a non-zero homomorphism then f is an isomorphism. If M is a simple module then $\operatorname{End}_R(M)$ is a division ring.*

Proof. Let $f : M \to N$ be a non-zero homomorphism. Then $\operatorname{Im} f \neq 0$ and $\ker f \neq M$. As 0 and M are the only submodules of M and 0 and N are the only submodules of N, we have $\operatorname{Im} f = N$ and $\ker f = 0$. Therefore f is bijective and hence it is invertible. □

An obvious consequence of the Schur Lemma (Lemma 4.1) is that if M and N are two simple modules then either $M \cong N$ or $\operatorname{Hom}_R(M, N)$.

4.2. Proposition *Let $M = \sum_{i=I}^{k} S_i$ with each S_i a simple submodule of M and let N be a submodule of M. Then*

1. *There is a subset J of I such that $M = N \oplus \oplus_{j \in J} S_j$. In particular, there is a submodule P of M such that $M = N \oplus P$.*
2. *There is a subset J of I such that $M = \oplus_{j \in J} S_j$.*
3. *Every simple submodule of M is isomorphism to some S_i.*
4. *N and M/N are semisimple.*
5. *A direct sum of semisimple modules is semisimple.*

Proof. 1. Let Σ be the set formed by the subsets J of I for which the family $\{N, S_j : j \in J\}$ is independent. This is set is inductive because the union of a totally ordered subset of Σ also belongs to Σ. By the Zorn's Lemma, Σ has a maximal element, say J. We claim that $M = N \oplus \oplus_{i \in J} S_j$. Otherwise there is some $i \in I$ such that $S_i \not\subseteq N \oplus \oplus_{i \in J} S_j$. As S_i is simple we have $S_i \cap (N \oplus \oplus_{i \in J} S_j) = 0$ and then it is easy to see that $J \cup \{i\}$ is a subset of Σ properly containing J. This contradicts the maximality of J and finishes the proof.

2 is a direct consequences of 1 for $N = 0$.

3. Let S be a simple submodule of M then $M = S \oplus P = P \oplus \oplus_{j \in J} S_j$ for some submodule P of M and some $J \subseteq I$. Then $S \cong M/P \cong \oplus_{j \in J} S_j$ and this implies that J has cardinality 1 and S is isomorphic to M_j if $J = \{j\}$.

4. Clearly $M/N = \sum_{i \in I} (N + S_i)/N$ and every $(N + S_i)/N$ is either 0 or simple. Eliminating the zero summands we deduce that M/N is semisimple. Moreover, by 1, $M = N \oplus P$ for some submodule P of M. Then $N \cong M/P$ and hence N is semisimple.

5 is obvious. □

Let M be a semisimple module. By Proposition 4.2.2, M is a direct sum of simple modules. We can group the direct summands by isomorphisms classes, so that $M \cong S_1^{m_1} \oplus \cdots \oplus S_k^{m_k}$ with $S_{i_1} \ncong S_{i_2}$ for $i_1 \neq i_2$. The following proposition describes isomorphism classes between semisimple modules.

4.3. Proposition *Consider semisimple modules*

$$M \cong M_1 \oplus \cdots \oplus M_m \quad \text{and} \quad N \cong N_1 \oplus \cdots \oplus N_n$$

where each M_i and each N_i is simple. Then $M \cong N$ if and only if $m = n$ and there is $\sigma \in S_m$ such that $M_i \cong N_{\sigma(i)}$.

Proof. The sufficient condition is clear. Suppose that M and N are isomorphic. We may assume without loss of generality that $0 \leq m \leq n$. We argue by induction on m. The case $m = 0$ is obvious. Suppose $m > 1$ and he induction hypothesis. Let $f : M \to N$ be an isomorphism. Let $\mu_i : M_i \to M$ and $\pi_i : N \to N_i$, the canonical embedding and projection. Let $M_i' = f^{-1}(M_i)$ for every $i = 1, \ldots, n$. Then $M = \prod_{i=1}^n M_i'$ and each M_i' is simple. Moreover, by Proposition 4.2.1, there is $J \subseteq \{1, \ldots, m\}$ such that $M = \oplus_{i=1}^{n-1} M_j' \oplus \oplus_{j \in J} M_j$. Then $M_n' \cong M/ \oplus_{i=1}^{n-1} M_i' \cong \oplus_{j \in J} M_j$. As M_n' is simple, $|J| = 1$. By permuting the N_j one may assume that $J = \{m\}$. Then $N_n \cong M_n' \cong M_m$ and $M/ \oplus_{i=1}^{n-1} M_i' \cong M/M_m \cong \oplus_{i=1}^{m-1} M_i$. By the induction hypothesis $m - 1 = n - 1$ and after a permutation one may assume that $N_i \cong M_i' \cong M_i$ for every i. □

Proposition 4.3 also holds for semisimple modules which are infinite direct sums of simple modules (see e.g. [Pie82, 2.5]). This shows that if $\{S_i : i \in I\}$ is a set of representatives of the isomorphism classes of simple right R-modules, then every semisimple right R-module M has a unique expression as $M \cong \oplus_{i \in I} S_i^{(\alpha_i)}$ for some cardinals α_i. Then α_i is called the the *multiplicity* of S_i at M.

4.4. Theorem [The Wedderburn-Artin Theorem] *The following conditions are equivalent for a ring:*

1. *The left module ${}_RR$ is semisimple.*
2. *The right module R_R is semisimple.*
3. *There are division rings $D_1, \ldots, D_k$ and positive integers $n_1, \ldots, n_k$ such that*

$$R \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k). \tag{4.9}$$

Proof. 3 implies 1 and 2. Suppose that $R = M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$ with D_i a division ring and n_i a positive integer for every $i = 1, \ldots, k$. For every $i = 1, \ldots, k$ and every $j = 1, \ldots, n_i$ let C_{ij} be the subset of R formed by the elements for which all the non-zero entries are at the j-th column of $M_{n_i}(D_i)$ and let R_{ij} be the subset formed by the elements of R with all the non-zero entries are at the j-th row of $M_{n_i}(D_i)$. It is easy to see that $R = \oplus_{i=1}^k \oplus_{j=1}^{n_i} C_{ij} = \oplus_{i=1}^k \oplus_{j=1}^{n_i} R_{ij}$, that each C_{ij} is a minimal left ideal of ${}_RR$ and R_{ij} is a minimal right ideal of R_R. Thus ${}_RR$ and R_R are semisimple. This proves that 3 implies 1 and 2.

2 implies 3 and 1 implies 3. By symmetry we only prove the first. Suppose that R_R is semisimple. By Proposition 4.2.2, $R_R = \oplus_{i \in I} S_i$ for some simple right ideals of R. We claim that I is finite. Indeed, there is a finite subset J of I such that $1 = \sum_{i \in J} s_j$. If $s \in S_i$ with $i \notin J$ then $s = 1s = \sum_{j \in J} s_j s \in S \cap \sum_{j \in J} S_j = 0$. Thus $S_i = 0$, which yields a contradiction because S_j is simple. This shows that $J = I$, so that I is finite, as claimed. Grouping the S_i which are isomorphic we have $R_R = \oplus_{i=1}^k M_i$ and $M_i = \oplus_{j=1}^{n_i} T_{ij}$ with each R_{ij} a simple right ideal of R and $T_{i_1 j_1} \cong T_{i_2 j_2}$ if and only if $i_1 = i_2$. Thus, if $T_i = T_{i1}$, then

$$\mathrm{Hom}_R(T_{i_1 j_1}, T_{i_2 j_2}) \cong \begin{cases} 0, & \text{if } i_1 \neq i_2; \\ \mathrm{End}_R(T_i) = D_i & \text{if } i_1 = i_2 = i; \end{cases}$$

and each D_i is a division ring by the Schur's Lemma (Lemma 4.1). By (2.5), we have

$$\mathrm{Hom}_R(M_i, M_j) = \begin{cases} 0, & \text{if } i \neq j; \\ \mathrm{End}_R(M_i) \cong \mathrm{End}_R(T_i^{n_i}) \cong M_{n_i}(D_i) & \text{if } i = j. \end{cases}$$

By (2.4),

$$R \cong \mathrm{End}(R_R) \cong \begin{pmatrix} \mathrm{Hom}_R(M_1, M_1) & \mathrm{Hom}_R(M_2, M_1) & \ldots & \mathrm{Hom}_R(M_k, M_1) \\ \mathrm{Hom}_R(M_1, M_2) & \mathrm{Hom}_R(M_2, M_2) & \ldots & \mathrm{Hom}_R(M_k, M_l) \\ \ldots & \ldots & \ldots & \ldots \\ \mathrm{Hom}_R(M_1, M_k) & \mathrm{Hom}_R(M_2, M_k) & \ldots & \mathrm{Hom}_R(M_k, M_l) \end{pmatrix} = \prod_{i=1}^k M_{n_i}(D_i).$$

□

If R_R (equivalently ${}_RR$) is semisimple then we say that R is a *semisimple ring*. If R is a semisimple ring then the expression of R as in (4.9) is called the *Wedderburn decomposition* of R. The direct factors $M_{n_i}(D_i)$ are called the *Wedderburn components* of R. The proof of Theorem 4.4 shows that if the Wedderburn decomposition of R is as in Theorem 4.4.3 then R has exactly k simple left R-modules up to isomorphism and k simple right R-modules up to isomorphisms. Moreover, one can take $C_1, \ldots, C_k$ as representatives of the simple left R-modules, where each C_i is one column of $M_{n_i}(D_i)$. Similarly, taking one row R_i of each Wedderburn component $M_{n_i}(D_i)$, we obtain a set $R_1, \ldots, R_k$ of representatives of the simple right R-modules. Moreover ${}_RR \cong \oplus_{i=1}^k C_i^{n_i}$ and $R_R \cong \oplus_{i=1}^k R_i^{n_i}$.

In case R is finite the all the division rings are finite and hence they are fields by the following well known theorem of Wedderburn.

4.5. Theorem [Wedderburn] *Every finite division ring is a field.*

Suppose that R is a semisimple ring. The proof of Theorem 4.4, as well as Proposition 4.2.3 shows that if $S_1, \ldots, S_k$ are representatives of the minimal right ideals up to isomorphisms then $R \cong S_1^{n_1} \oplus \cdots \oplus S_k^{n_k}$ for some unique positive integers $n_1, \ldots, n_k$. Furthermore R has exactly k isomorphism classes of minimal left ideals, say $T_1, \ldots, T_k$ and $R \cong T_1^{n_1} \oplus \cdots \oplus T_k^{n_k}$ (for the same positive integers). Moreover, every right R-module is a direct sum of copies of S_i's and every left R-module is a direct sum of T_j's. This is clear for free modules and then it is true for all modules because every module is a quotient of a free module. This proves

4.6. Corollary *If R is a semisimple ring then every R-module is semisimple and every right (left) simple module is isomorphic to a minimal right (left) ideal of R.*

5. The socle and the Jacobson radical

Let M be a module. The *socle* of M, denoted $\mathrm{Soc}(M)$, is the sum of all simple submodules of M. Clearly $\mathrm{Soc}(M)$ is the unique maximal semisimple submodule of M. In general, it could occur that $\mathrm{Soc}(M) = 0$ but in this case M must be infinite.

Let N be a submodule of M. The the map $K \mapsto K/N$ gives a one-to-one correspondence from the set of submodules of M containing N to the submodules of M/N. Then M/N is simple if and only if N is a *maximal submodule* of M, i.e. N and M are different and they are the only submodules of M containing N. The annihilator of M is

$$\mathrm{Ann}(M_R) = \{r \in R : Mr = 0\}.$$

Clearly $\mathrm{Ann}(M_R)$ is an ideal of R. Therefore if $\mathcal{S}_r$ denotes the class of all simple right R-modules of R then

$$rad(R_R) = \bigcap_{S \in \mathcal{S}_r} \mathrm{Ann}(S_R)$$

is a two-sided ideal of R. Similarly

$$rad({}_R R) = \bigcap_{S \in \mathcal{S}_l} \mathrm{Ann}(S_R)$$

where $\mathcal{S}_l$ denotes the class of simple left R-modules. Actually, $rad(R_R) = rad({}_R R)$ (see [Pie82, Proposition 4.3]). This ideal is called the *Jacobson radical* of R and it is usually denoted $J(R)$. If M is a semisimple right R-module then $MJ(R) = 0$ and hence we can see M as a right $R/J(R)$-module.

We can give an alternative description of $J(R)$. If M is a module then a *maximal submodule* of M is a submodule N of M which is maximal among the submodules of M different from M. By Examples 2.1.3, N is a maximal submodule of M if and only if M/N is simple. The *maximal right ideals* of R are the maximal submodules of R_R. Maximal left ideals are defined similarly.

5.1. Proposition *$J(R)$ is the intersection of the maximal left ideals of R and it is also the intersection of the right ideals of R.*

Proof. By symmetry it is enough to prove the first statement. Let J be the intersection of the maximal right ideals of R. Let M be a maximal right ideal of R. Then $S = R/M$ is a simple right R-module. Therefore $0 = SJ(R) = (M + J(R))/M$ and therefore $J(R) \subseteq M$. This shows $J(R) \subseteq J$.

If S is a simple right R-module and $s \in S \setminus \{0\}$ then $S = sR$ and hence the maps $\rho_s : R \to S$, associating r with sr, is surjective. Thus $S \cong R/\ker \rho_s$ and hence $\ker \rho_s$ is a maximal ideal of M. Thus $J \subseteq \ker \rho_s$ and hence $SJ = 0$. This shows $J \subseteq J(R)$. □

It is easy to see that if R is semisimple then $J(R) = 0$. Furthermore, by the description of left and right ideals of $R/J(R)$ it is clear that $J(R/J(R)) = 0$. For finite rings we have

5.2. Proposition *If R is a finite ring then R is semisimple if and only if $J(R) = 0$. In particular $R/J(R)$ is semisimple.*

Proof. Suppose that $J(R) = 0$. Then there are maximal right ideals $I_1, \ldots, I_k$ of R with $I_1 \cap \cdots \cap I_k = 0$. Then the map $r \to (r + I_1, \ldots, r + I_k)$ is an injective homomorphism $R \to \oplus_{i=1}^k R/I_i$. As each R/I_i is simple, we deduce that R is semisimple by Proposition 4.2. □

5.3. Remark *Assume that I is an ideal of R with R/I semisimple. Then $J(R/I) = 0$ and hence the intersection of the maximal ideals of R containing I is precisely I. Therefore $J(R) \subseteq I$.*

5.4. Example *Let F be a field and consider the ring $R = \begin{pmatrix} F & F \\ 0 & F \end{pmatrix}$ of upper triangular 2×2 matrices. Then $J(R) = \begin{pmatrix} 0 & F \\ 0 & 0 \end{pmatrix}$, $\mathrm{Soc}(R_R) = \begin{pmatrix} 0 & F \\ 0 & F \end{pmatrix}$ and $\mathrm{Soc}({}_RR) = \begin{pmatrix} F & F \\ 0 & 0 \end{pmatrix}$*

Proof. Clearly, $I_1 = \begin{pmatrix} F & F \\ 0 & 0 \end{pmatrix}$ and $I_2 = \begin{pmatrix} 0 & F \\ 0 & F \end{pmatrix}$ are maximal right ideals of R. Therefore $J = \begin{pmatrix} 0 & F \\ 0 & 0 \end{pmatrix} \subseteq J(R)$. On the other hand $R/J \cong F \times F$, which is semisimple. Thus $J = J(R)$ by Remark 5.3.

Clearly $J(R)$ is a minimal left ideal and a minimal right ideal. Moreover, $J_1 = \begin{pmatrix} F & 0 \\ 0 & 0 \end{pmatrix}$ is a minimal left ideal and $J_2 = \begin{pmatrix} 0 & 0 \\ 0 & F \end{pmatrix}$ a minimal right ideal. Therefore $I_1 = J_1 + J(R) \subseteq \mathrm{Soc}({}_RR)$ and $I_2 = J_2 + J(R) \subseteq \mathrm{Soc}(R_R)$. As R is not semisimple and I_1 and I_2 are maximal we deduce that $I_1 = \mathrm{Soc}({}_RR)$ and $I_2 = \mathrm{Soc}(R_R)$. □

By Example 2.1.2, the right $R/J(R)$-modules can be identified with the right R-modules M such that $MJ(R) = 0$ and these are precisely the semisimple modules of R. Thus, the number of isomorphism classes of right R-modules coincides with the number of isomorphisms classes of right $R/J(R)$ which is also the number of simple components of $R/J(R)$. Using this it is easy to prove the following

5.5. Lema *Let R be a finite ring and let M be a semisimple module. Then M is cyclic if and only if for every simple R-module S, the multiplicity of S in M is at most the multiplicity of S in $R/J(R)$.*

5.6. Lemma *If R is a finite ring and M is a finite non-zero right R module then $MJ(R) \neq M$.*

Proof. As M is finite, it has a maximal submodule N (i.e. a submodule maximal among the submodules different from M). Then M/N is simple and hence $(M/N)J(R) = 0$. Therefore $MJ(R) \subseteq N \subset M$[1] and therefore $MJ(R) \neq 0$. □

The following is an obvious consequence of Lemma 5.6.

5.7. Corollary *If R is a finite ring then $J(R)^n = 0$ for some n.*

Let R be a finite ring and let $x \in R$ such that $x^n = 0$ for some $n \geq 1$. Then $(1+x)(1-x+x^2-\cdots+(-1)^{n-1}x^{n-1}) = 1$, so that $1 + x \in \mathcal{U}(X)$. If $u \in \mathcal{U}(R)$ and $x \in J(R)$ then $u^{-1}x \in J(R)$ and therefore $(u^{-1}x)^n = 0$ for some n. Therefore $u + x = u(1 + u^{-1}x) \in \mathcal{U}(R)$. This shows that

$$\mathcal{U}(R) + J(R) \subseteq \mathcal{U}(R). \tag{5.10}$$

6. Injective modules

Let R be a ring and let E be and M be a R-modules. We say that E is *M-injective* if for every submodule N of M and every homomorphism $f : N \to E$ there is a homomorphism $\overline{f} : M \to E$ extending f, i.e. $\overline{f}(n) = f(n)$ for every $n \in N$. One says that E is injective if it is M-injective for every module M.

6.1. Proposition *Let $\{E_i : i \in I\}$ be a family of modules and let M be a module. Then $\prod_{i\in I} E_i$ is M-injective if and only if E_i is M-injective for every $i \in I$.*

Proof. Let $E = \prod_{i\in I} E_i$.

Suppose that each E_i is M-injective. Let N be a submodule of a module M and let $f : N \to E$ be a homomorphism. For every $i \in I$ let $\pi_i : E \to E_i$ be the projection on the i-th coordinate and let $f_i = \pi_i f$. As E_i is injective there is a homomorphism $g_i : M \to E_i$ such that $g_i(n) = \pi_i f(n)$ for every $n \in N$. Let $g : M \to E$ be the unique homomorphism satisfying $\pi_i g = g_i$ for every i. Then $\pi_i g(n) = g_i(n) = \pi_i f(n)$ for every $n \in N$ and hence $g(n) = f(n)$ for every $n \in N$. This shows that E is M-injective.

Conversely, assume that E is M-injective and let $f : N \to E_i$ be a homomorphism. Let $\mu_i : E_i \to E$ be the natural embedding of E_i into the i-th coordinate of E. As E is M-injective Then there is a homomorphism $g : M \to E$ such that $g(n) = \mu_i f(n)$. Then $\pi_i g(n) = \pi_i \mu_i f(n) = f(n)$. Thus E_i is N-injective. □

6.2. Proposition *Let E be a module.*

1. *If E is M-injective and N is a submodule of M then E is M/N-injective.*
2. *Let $\{M_i : i \in I\}$ be a family of modules. If E is M_i-injective for every $i \in I$ and every $j \in J$ then E is $\oplus_{i\in I} M_i$-injective.*

[1] $\subset$ denotes proper inclusion.

Proof. 1. Suppose that E is M-injective. Every submodule of M/N is of the form K/N for some submodule K of M containing N. Let $f : K/N \to M$ be a homomorphism with K as above. Let $\pi : M \to M/N$ be the canonical homomorphism and let $\pi_K : K \to K/N$ denote its restriction to K. As E is M-injective, there is a homomorphism $g : M \to E$ with $g(k) = f\pi_K(k)$ for every $k \in K$. Then $f(N) = 0$ and hence there is a homomorphism $\overline{g} : M/N \to E$ with $\overline{g}\pi = g$. Therefore $\overline{g}(k+N) = \overline{g}\pi_K(k) = g(k) = f\pi_K(k) = f(k+N)$ for every $k \in K$. This shows that E is M/N-injective.

2. Suppose that E is M_i-injective for every $i \in I$. Let $M = \oplus_{i\in I} M_j$, let N be a submodule of M and let $f : N \to E$ be a homomorphism. Using Zorn's Lemma we may assume that N is maximal in the set of submodules of N_1 of $\oplus_{i\in I} M_i$ for which there is a homomorphism $N_1 \to E$ extending f. It is then enough to show that under this maximality assumption $N = M$. By means of contradiction we assume that $N \neq M$.

For every $i \in I$ let $\mu_i : M_i \to M$ be the embedding of M_i into the i-th coordinate. As $N \neq M$ there is $j \in I$ such that $\mu_j(M_j) \not\subseteq N$. Let $g : \mu_j^{-1}(N) \to E$ be given by $g(m) = f\mu_j(m)$ for $m \in \mu_j^{-1}(N)$. By assumption, there is $h : M_j \to E$ such that $h(m) = g(m)$ for every $m \in \mu_j^{-1}(N)$. Let $h_1 : N_1 = N + \mu_j(M_j) \to E$ be defined by

$$h_1(n + \mu_j(m)) = f(n) + h(m), \quad (n \in N, m \in M_j).$$

This is well defined because if $n_1 + \mu_j(m_1) = n_2 + \mu_j(m_2)$, with $n_1, n_2 \in N$ and $m_1, m_2 \in K$ then $n_1 - n_2 = \mu_j(m_2 - m_1) \in N$ and hence $m_2 - m_1 \in \mu_j^{-1}(N)$. Then $f(n_1) - f(n_2) = f(n_1 - n_2) = f\mu_j(m_2 - m_1) = g(m_2 - m_1) = h(m_2 - m_1) = h(m_2) - h(m_1)$ and hence $f(n_1) + h(m_1) = f(n_2) + h(m_2)$. As h_1 extends f and N is properly contained in N_1, we obtain the desired contradiction from the maximality assumption. □

6.3. Theorem [Baer's Criterion of Injectivity] *Let R be a ring and let E be a right R-module. Then E is injective if for every ideal I of R and every homomorphism $f : I \to E$ there is $m \in M$ such that $f(x) = mx$ for every $x \in I$.*

Proof. Every homomorphism $R_R \to M$ is of the form $r \mapsto mr$ for some $m \in M$. Thus the property that for every ideal I of R and every homomorphism $f : I \to E$ there is $m \in m$ such that $f(x) = mx$ for every $x \in I$ means precisely that E is R-injective. Then, by Proposition 6.2, E is M injective for every quotient M of every free module. As every module is of this form we deduce that E in injective. □

Applying Baer's Criterion to the case where $R = \mathbb{Z}$ we obtain the following:

6.4. Corollary *A $\mathbb{Z}$-module (i.e. an abelian group) M is injective if for every $m \in M$ and every positive integer n there is $n \in M$ with $m = dn$.*

Using Corollary 6.4 we deduce.

6.5. Example *$\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$ are injective $\mathbb{Z}$-modules.*

If $f : M \to N$ is a homomorphism of modules and E is a module then the following map is a homomorphism of abelian groups:

$$\begin{array}{rcl} \mathrm{Hom}(f, E) : \mathrm{Hom}_R(N, E) & \to & \mathrm{Hom}_R(M, E) \\ \phi & \mapsto & \phi \circ f. \end{array}$$

$\mathrm{Hom}(-, E)$ defines a contravariant functor from the category of modules to the category of abelian groups, i.e.

$$\mathrm{Hom}(g \circ f, E) = \mathrm{Hom}(f, E) \circ \mathrm{Hom}(g, E) \quad \text{and} \quad \mathrm{Hom}(1_M, E) = 1_{\mathrm{End}_R(M)}$$

for every module M and every "composable" homomorphisms f and g. A sequence of homomorphisms of modules

$$\cdots \to M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \to \dots$$

is said to be exact if $\ker f_i = \mathrm{Im}\ f_i$ for every i. For example, if $f : M \to N$ is a homomorphism, then f is injective if and only if $0 \to M \xrightarrow{f} N$ is exact. Similarly f is surjective if $M \xrightarrow{f} N \to 0$ is exact. A *short exact sequence* is an exact sequence of the form

$$0 \to M' \to M \to M'' \to 0$$

6.6. Proposition *If*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

is a short exact sequence then

$$0 \to \mathrm{Hom}_R(M'', E) \xrightarrow{\mathrm{Hom}(g,E)} \mathrm{Hom}_R(M, E) \xrightarrow{\mathrm{Hom}(f,E)} \mathrm{Hom}_R(M', E)$$

is exact.

Proof. As g is surjective, if $g \circ \phi = g \circ \psi$ then $\phi = \psi$. This shows that $\mathrm{Hom}(g, E)$ is injective. Moreover $\mathrm{Hom}(f, E) \circ \mathrm{Hom}(g, E) = \mathrm{Hom}(g \circ f, E) = \mathrm{Hom}(0, E) = 0$ and therefore $\mathrm{Im}\ \mathrm{Hom}(g, E) \subseteq \ker \mathrm{Hom}(f, E)$. Assume that $\phi \in \ker \mathrm{Hom}(f, E)$. Then $\phi \circ f = 0$, and therefore $\ker g \subseteq \mathrm{Im}\ f \subseteq \ker \phi$. Thus the map $\psi : M'' \to E$ given by $\psi(x) = \phi(y)$ if $x = g(y)$ is a well defined homomorphism. Indeed, if $x = g(y_1) = g(y_2)$ then $y_1 - y_2 \in \ker g \subseteq \ker \phi$ and hence $\phi(y_1) = \phi(y_2)$. It follows easily that $\psi \in \mathrm{Hom}_R(M'', E)$ and $\phi = \psi \circ g$. This shows that $\phi \in \mathrm{Im}\ \mathrm{Hom}(g, E)$ and finishes the proof. □

By Proposition 6.6, E is injective if and only if $\mathrm{Hom}(f, E)$ is surjective for every injective homomorphism f or R-modules if and only if $\mathrm{Hom}(-, E)$ maps short exact sequences to short exact sequences.

Given an abelian group A let $A^* = \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$ and given a homomorphism f of abelian groups let $f^* = \mathrm{Hom}(f, \mathbb{Q}/\mathbb{Z})$. For every abelian group A, A^* is an abelian group and for every homomorphism f of abelian groups, f^* is s group homomorphism.

In case R is a ring and M is right R-module then, considering M as an $(\mathbb{Z}, R)$-bimodule, we can see M^* is a left R-module (see Examples 2.1.7). Similarly if M is a left R-module then M^* as a right R-module. If f is a homomorphism of modules then so is f^*. Clearly R^* is an (R, R)-bimodule.

6.7. Lemma *For every R-module there is an isomorphism of abelian groups $\Phi_M : \mathrm{Hom}_R(M, R^*) \to M^*$ such that if $f : M \to N$ is a homomorphism of R-modules then the following diagram is commutative*

$$\begin{array}{ccc} \mathrm{Hom}_R(N, R^*) & \xrightarrow{\mathrm{Hom}(f, R^*)} & \mathrm{Hom}_R(M, R^*) \\ \Phi_N \downarrow & & \downarrow \Phi_M \\ N^* & \xrightarrow{f^*} & M^* \end{array}$$

Proof. We define Φ_M by setting $\Phi_M(f)(m) = f(m)(1)$ for $m \in M$ and $f \in \mathrm{Hom}_R(M, R^*)$. We also define $\Psi_M : M^* \to \mathrm{Hom}_R(M, R^*)$, by setting $\Phi(g)(m)(r) = g(mr)$ for $m \in M$, $r \in R$ and $g \in M^*$. The reader can easily check that Φ_M and Ψ_M are homomorphisms, that they are inverse to each other and that the diagram is commutative. □

6.8. Proposition *If R is a ring then R^* is injective as left and right module.*

Proof. By symmetry it is enough to prove the right version. Consider a short exact sequence of right R-modules

$$0 \to M_1 \to M \to M_2 \to 0$$

By Lemma 6.7 we have a commutative diagram which vertical isomorphisms

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{Hom}_R(M_2, R^*) & \to & \mathrm{Hom}_R(M, R^*) & \to & \mathrm{Hom}_R(M_1, R^*) & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & M_2^* & \to & M^* & \to & M_1^* & \to & 0 \end{array}$$

By Example 6.5, $\mathbb{Q}/\mathbb{Z}$ is injective as abelian group and hence the lower sequence of the diagram is exact. Then the upper sequence is exact too. This shows that R^* is injective as right R-module. □

The following proposition shows a connection between the EP and a condition closely related to injectivity.

6.9. Proposition [DLP04] *Let R be a finite ring and let M be a finite module. Then the following conditions are equivalent.*

1. *M has the EP for length 1.*
2. *Every isomorphism $f : C_1 \to C_2$ for C_1 and C_2 linear codes of length 1 in the alphabet M extends to an automorphism of M.*
3. *Every injective homomorphisms $C \to M$ for C a submodule of M extends to an automorphism of M.*
4. *Every injective homomorphisms $C \to M$ for C a submodule of M extends to an endomorphism of M.*

Proof. $1 \Leftrightarrow 2 \Leftrightarrow 3 \Rightarrow 4$ are all obvious.

$4 \Rightarrow 3$. Suppose that M satisfies condition 4 and let $f : C \to M$ be an injective homomorphism with C a submodule of M. Then $\mathrm{Soc}(M)$ is semisimple and $\mathrm{Soc}(C)$ is a submodule of $\mathrm{Soc}(M)$. Then, by Proposition 4.2.1, $\mathrm{Soc}(M) = \mathrm{Soc}(C) \oplus N$ for some submodule N of $\mathrm{Soc}(M)$. As $\mathrm{Soc}(M)$ is semisimple, so is N and hence $N \cap C \subset N \cap \mathrm{Soc}(M) = 0$. Therefore there is a unique homomorphism $f_1 : C_1 = C \oplus N \to M$ with such that f_1 acts as the f on C and as the identity on N. By hypothesis f_1 extends to an endomorphism g of M. Then $\mathrm{Soc}(\ker g) \subseteq \mathrm{Soc}(M) \cap \ker g = \mathrm{Soc}(C_1) \cap \ker g \subseteq C_1 \cap \ker g = 0$. Then $\mathrm{Ker}\ g = 0$, because $\ker g$ is finite. Therefore g is an injective endomorphism of M. As M is finite g is also surjective and hence g is an automorphism. □

A module M satisfying the conditions of Proposition 6.9 is said to be *pseudoinjective*.

7. Characters of finite abelian groups

In this section A is a finite abelian group which we denote additively. Recall that $A^* = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})(= \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$. Moreover, for a homomorphism of abelian groups $f : A \to B$ let $f^* = \mathrm{Hom}_{\mathbb{Z}}(f, \mathbb{Q}/\mathbb{Z}) : B^* \to A^*$.

7.1. Proposition *Let A and B be finite abelian groups. Then*

1. *There is an isomorphism $\lambda : A \to A^*$ satisfying*

$$\lambda(a)(b) = \lambda(b)(a) \quad (a, b \in A). \tag{7.11}$$

Hence $|A| = |A^*|$.

2. *The map $\Phi_A : A \to A^{**}$ defined by*

$$\Phi_A(a)(\chi) = \chi(a) \quad (a \in A, \chi \in A^*).$$

is a group isomorphism such that for every homomorphism of abelian groups $f : A \to B$ the following diagram is commutative:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \Phi_A \downarrow & & \downarrow \Phi_B \\ A^{**} & \xrightarrow{f^{**}} & B^{**} \end{array}$$

Proof. 1. Assume first that A is cyclic. Then $A \cong \mathbb{Z}/n\mathbb{Z}$ for some non-negative integer n and we may assume without loss of generality that $A = \mathbb{Z}/n\mathbb{Z}$. Then, the map $\lambda : A \to A^*$ given by $\lambda(i + n\mathbb{Z})(j + n\mathbb{Z}) = \frac{ij}{n} + \mathbb{Z}$ is an injective group homomorphism satisfying (7.11). If $\chi \in A^*$ then χ is determined by $\chi(1)$. As $n1 = 0$, necessarily $n\chi(1) = 0$ and hence $\chi(1) = \frac{i}{n} + \mathbb{Z}$ for some integer $i = 0, 1, \ldots, n-1$. Then $\chi(j + n\mathbb{Z}) = j\chi(1 + n\mathbb{Z}) = j(\frac{i}{n} + \mathbb{Z}) = \frac{ij}{n} + \mathbb{Z} = \lambda(i + n\mathbb{Z})(j + n\mathbb{Z})$. Thus $\chi = \lambda(i + n\mathbb{Z})$. This shows that λ is surjective and therefore it is an isomorphism.

Suppose now that A and B are two finite abelian groups and $\lambda_A : A \to A^*$ and $\lambda_B : B \to B^*$ are isomorphisms satisfying (7.11). Then $\lambda(a_1, b_1)(a_2, b_2) = \lambda_A(a_1)(a_2) + \lambda_B(b_1)(b_2)$ defines an isomorphism $\lambda : A \times B \to (A \times B)^*$ satisfying (7.11).

In the general case $A = A_1 \times \cdots \times A_k$, with each A_i cyclic. Arguing by induction on k with the conclusions of the two previous paragraphs we deduce that there is an isomorphism $\lambda : A \to A^*$ satisfying (7.11).

2. Proving that Φ_A is a group homomorphism and that the diagram is commutative is straightforward. To show that Φ is injective we write $A = \langle a_1 \rangle \times \cdots \times \langle a_k \rangle$, and assume that a_i has order d_i. If $0 \neq a \in A$ then $a = \sum_{i=1}^k e_i a_i$ with $0 \leq e_i < d_i$ and some $e_j \neq 0$. Then the map $\chi : A \to \mathbb{Q}/\mathbb{Z}$ associating $\sum_{i=1}^k x_i a_i$ with $\frac{x_j}{d_i} + \mathbb{Q}/\mathbb{Z}$ is an element of A^* with $\Phi(a)(\chi) = \chi(a) = \frac{e_i}{d_i} + \mathbb{Z} \neq 0$. Thus Φ is injective and hence it is a bijection because A and A^{**} have the same cardinality, by 1. □

So far we have used additive notation for all the abelian groups. However we need now to use the multiplicative group $\mathcal{U}(\mathbb{C})$ and we use also multiplicative notation for the group $\mathrm{Hom}(A, \mathcal{U}(\mathbb{C}))$, so that if $f, g \in \mathrm{Hom}(A, \mathcal{U}(\mathbb{C}))$ and $a \in A$ then $(fg)(a) = f(a)g(a)$. The map $x \mapsto e^{2\pi i x}$ is a group homomorphism from the additive group of $\mathbb{Q} \to \mathcal{U}(\mathbb{C})$. The kernel of this homomorphism is $\mathbb{Z}$ and hence it induces an injective homomorphism

$$\Phi : (\mathbb{Q}/\mathbb{Z}, +) \to \mathcal{U}(\mathbb{C}).$$

Therefore we have a group homomorphism

$$\begin{array}{rcl} \Phi_* : A^* = \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z}) & \to & \mathrm{Hom}(A, \mathcal{U}(\mathbb{C})) \\ f & \mapsto & f_* = \Phi \circ f \end{array}$$

We claim that Φ_* is an isomorphism. Indeed, if $\chi \in \mathrm{Hom}(A, \mathcal{U}(\mathbb{C}))$ then $\mathrm{Im}\ \chi \subseteq \mathrm{Im}\ \Phi =$ Set of roots of unity of $\mathbb{C}$. As Φ is injective, there is a unique $f \in \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$ with $\chi = \Phi \circ f = f_*$.

Let $\mathbb{C}^A$ be the set of maps $A \to \mathbb{C}$ endowed with a structure of vector space over $\mathbb{C}$ with the Hermitian product

$$\langle f, g \rangle = \frac{1}{|A|} \sum_{a \in A} f(a)\overline{g(a)}.$$

In particular the elements of the form ϕ_* with $\phi \in A^*$ belong to $\mathbb{C}^*$.

7.2. Proposition *Let A be a finite abelian group. Then*

1. *If $\chi \in A^*$ then*

$$\sum_{a \in A} \chi_*(a) = \begin{cases} |A|, & \text{if } \chi = 0; \\ 0, & \text{otherwise.} \end{cases}$$

2. If $a \in A$ then

$$\sum_{\chi \in A^*} \chi_*(a) = \begin{cases} |A|, & \text{if } a = 0; \\ 0, & \text{otherwise.} \end{cases}$$

3. $\{\chi_* : f \in A^*\}$ is an orthonormal basis of $\mathbb{C}^G$.

Proof. 1. Let $\chi \in A^*$. If $\chi = 0$ then $\chi_*(a) = 1$ for every $a \in A$ and hence $\sum_{a\in A} \chi_*(a) = |A|$. Suppose otherwise that $\chi \neq 0$. As $\chi_*(A)$ is a finite subgroup of a field, it is cyclic, say generated by $\zeta = \chi_*(b)$, and suppose that ζ has order n. Then $n > 1$, because $\chi \neq 0$, and hence $\sum_{i=1}^{n} \zeta^i = 0$. Moreover, $[A : \ker \chi] = n$ and $0, b, 2b, \ldots, (n-1)b$ is a set of representatives of $A/\ker \chi$. Therefore, every element of A has the form $ib + c$ with $i = 0, 1, \ldots, n-1$ and $c \in \ker \chi$. Thus

$$\sum_{a\in A} \chi(a) = \sum_{i=0}^{n-1} \sum_{c \in \ker \chi} \chi(ia + c) = |\ker \chi| \sum_{i=0}^{n-1} \zeta^i = 0.$$

2. Let $a \in A$. Let $\Phi : A \to A^{**}$ be the isomorphism of the proof of Proposition 7.1.2. Then $\Phi(a) = 0$ if and only if $a = 0$. By 1, applied to A^* we have

$$\sum_{\chi \in A^*} \chi_*(a) = \sum_{\chi \in A^*} \Phi(a)_*(\chi) = \begin{cases} |A^*| = |A|, & \text{if } a = 0; \\ 0, & \text{otherwise.} \end{cases}$$

3. Let $\chi, \phi \in A^*$. As $\phi_*(a)$ is a root of unity, $\overline{\phi_*(a)} = \phi_*(a)^{-1}$. As the map $\chi \mapsto \chi_*$ is a group homomorphism form the additive group of A^* to the multiplicative group $\mathrm{Hom}(A, \mathcal{U}(\mathbb{C}))$, we have $\langle \chi_*, \phi_* \rangle = \frac{1}{|A|} \sum_{a\in A} \chi_*(a)\phi_*(a)^{-1} = \frac{1}{A} \sum_{a\in A} (\chi - \phi)_*(a)$. Then, by 1,

$$\langle \chi_*, \phi_* \rangle = \begin{cases} 1, & \text{if } \chi = \phi; \\ 0, & \text{otherwise.} \end{cases}$$

This shows that the elements of $\{\chi_* : \chi \in A^*\}$ are orthonormal. As its cardinality coincides with the dimension of $\mathbb{C}^A$ they form an orthonormal basis. □

Let B be a subgroup of A and let $\pi : A \to A/B$ be the natural homomorphism. If $\phi \in (A/B)^*$ then $\phi \circ \pi \in A^*$. Moreover, $\phi \mapsto \phi \circ \pi$ defines an injective group homomorphism $(A/B)^* \to A^*$ whose image is

$$(A^* : B) = \{\chi \in A^* : B \subseteq \ker \chi\}.$$

Therefore

$$(A/B)^* \cong (A^* : B).$$

Thus, $B \neq 0$ if and only if $|A/B| < |A|$ if and only if $|(A^* : B)| < |A^*|$ if and only if $B \not\subseteq \ker \chi$ for some $\chi \in A^*$. This proves the following:

7.3. Lemma *Let A be a finite abelian group and let B be a subgroup of A. Then $B \neq 0$ if and only if $\chi(B) \neq 0$ for some $\chi \in A^*$.*

Recall that if R is a ring then R^* is an (R, R)-bimodule.

7.4. Lemma *Let R be a finite ring and let $r \in R$. Then $r = 0$ if and only if $rR^* = 0$ if and only if $R^*r = 0$.*

Proof. By Lemma 7.3, $rR^* = 0$ if and only if $\chi(Rr) = 0$ for every $\chi \in R^*$ if and only if $Rr = 0$ if and only if $r = 0$. Similarly $R^*r = 0$ if and only if $r = 0$. □

8. The Extension Property for module alphabets

Let R be a finite ring. A *Frobenius R-bimodule* is an (R, R)-bimodule M such that ${}_RM \cong {}_RR^*$ and $M_R \cong R^*_R$. Clearly R^* is a Frobenius R-bimodule. Let M be a Frobenius R-bimodule. Then $|M| = |R^*| = |R|$ and ${}_RM^* \cong_R R^{**} \cong_R R$ and $M^*_R \cong R_R$. Therefore M^* is cyclic both as left and right module. A *left (resp. right) generator* of M^* is an element $\chi \in M^*$ such that the unique homomorphism of left (resp. right) R-modules $R \to M^*$ mapping 1 to χ is an isomorphism. The following proposition characterizes the left and right generators of M.

8.1. Proposition *Let R be a finite ring, let M be a Frobenius R-bimodule and let $\chi \in M^*$. Then the following conditions are equivalent:*

1. χ is a left generator of M^*.
2. χ is a right generator of M^*.
3. $\ker \chi$ does not contain any non-zero submodule of ${}_RM$.
4. $\ker \chi$ does not contain any non-zero submodule of M_R.

Proof. Suppose that χ is not a left generator. Therefore the map $R \to M^*$ given by $r \mapsto r\chi$ is not an isomorphism. As R and M^* have the same cardinality this means that there is $r \in R \setminus \{0\}$ with $r\chi = 0$. Thus $\chi(Mr) = (r\chi)(M) = 0$. Therefore $Mr \subseteq \ker \chi$. Hence Mr is submodule of ${}_RM$ contained in $\ker \chi$. If $f : M \to R^*$ is an isomorphism then $R^*r = f(Mr)$. By Lemma 7.4, $R^*r \neq 0$ and hence Mr is a non-zero submodule of $\ker \chi$. This proves 3 implies 1. 4 implies 2 is proved similarly.

Suppose that χ is a left generator of M^* and let N be a submodule of M_R contained in $\ker \chi$. Let $\phi \in M^*$. As χ is a left generator there is $r \in R$ such that $\phi = r\chi$. Then $\phi(N) = (r\chi)(N) = \chi(Nr) = 0$. Therefore $N \subseteq \ker g$ for every $g \in M^*$. By Lemma 7.3, $N = 0$. This proves 1 implies 4. 2 implies 3 is proved similarly. □

8.2. Lemma *Let R be a finite ring and let M be a finite left R-module. Let $m_1, m_2 \in M$ such that $Rm_1 = Rm_2$. Then there is $u \in \mathcal{U}(R)$ such that $m_2 = um_1$.*

Proof. Suppose fits that $R = M_n(F)$ with R a field and let S be the first columns of R (i.e. the subset of R formed by the elements having all the non-zero entries in the first column). Then R is semisimple and S is the only simple left R-module up to isomorphisms. Then we may assume that $M = S^m$ for some positive integer m. Then we may identify M with $M_{n,m}(F)$ and in fact we may identify R with $\mathrm{End}(F_F^n)$ and M with $\mathrm{Hom}(F_F^m, F_F^n)$. The assumption $Rm_1 = Rm_2$ implies that m_1 and m_2 have the same image, say V. By the properties of vectors spaces there is a subspace W of F^n such that $F^n = V \oplus W$. Let u be the automorphism of F^n given by $um_1(x) = m_2(x)$ for every $x \in F^n$ and $u(w) = w$ for every $w \in W$. The reader should check that u is well define. Clearly $u \in \mathcal{U}(R)$ and $um_1 = m_2$.

Suppose next that R is semisimple. Then $R = M_{n_1}(F_1) \times \cdots \times M_{n_k}(F_k)$, with F_i a field for every i, by the Wedderburn-Artin Theorem (Theorem 4.4) and the Wedderburn Theorem (Theorem 4.5). Let e_i denote the identity of the i-component $M_{n_i}(F_i)$ of R. Then $1 = e_1 + \cdots + e_k$, $M = e_1M \oplus \cdots \oplus e_kM$ and each Me_i is a left Re_i-module (with $Re_i \cong M_{n_i}(F_i)$). As each e_i commutes with all the elements of R we have $Re_im_1 = e_iRm_1 = e_iRm_2 = Re_im_1$. By the previous case, for every $i = 1, \ldots, k$ there is $u_i \in \mathcal{U}(Re_i)$ with $u_ie_im_1 = u_ie_im_2$. Then $u = \sum_{i=1}^k u_i$ is a unit of R and $um_1 = \sum_{i=1}^k ue_im_1 = \sum_{i=1}^k u_ie_im_1 = \sum_{i=1}^k e_im_2 = m_2$, as desired.

Finally, consider the general case and consider $N = Rm_1/J(R)m_1$ as left $R/J(R)$-module. Then $R/J(R)(m_1 + J(R)m_1) = R/J(R)(m_2 + J(R)m_1)$ and hence there is $u_1 \in R$ and $x \in J(R)$ such that $m_2 - u_1m_1 = xm_1$ and $u_1 + J(R)$ is invertible in $R/J(R)$. Then $u_1u_2 = 1 + y$ with $y \in J(R)$ and hence $u_1 \in \mathcal{U}(R)$ and $u = u_1 + x \in \mathcal{U}(R)$, by (5.10), and $m_2 = um_1$. □

8.3. Theorem [GNW04] *Let R be a finite ring and let M be a Frobenius R-bimodule. Then M_R has the EP.*

Proof. Let C_1 and C_2 be linear codes of M_R^n and let $f : C_1 \to C_2$ be an isomorphism preserving the Hamming weight. Let $\pi_i : M^n \to M$ be the projection onto the i-th component for $i = 1, \ldots, n$ and let λ_i be the restriction of π_i to C_1 and μ_i the restriction of $\lambda_i f$ to C_1. By Proposition 7.2.1, for every $x \in C_1$, we have

$$\sum_{i=1}^{n} \sum_{\chi \in M^*} \chi_*(\lambda_i x) = |M| w(x) = |M| w(fx) = \sum_{i=1}^{n} \sum_{\chi \in M^*} \chi_*(\lambda_i f x) = \sum_{i=1}^{n} \sum_{\chi \in M^*} \chi_*(\mu_i x). \tag{8.12}$$

Let ϕ be a right generator of M^*. Then (8.12) can be rewritten as $\sum_{i=1}^n \sum_{r \in R} (\phi r)_*(\lambda_i x) = \sum_{i=1}^n \sum_{r \in R} (\phi r)_*(\mu_i x)$ or equivalently

$$\sum_{i=1}^{n} \sum_{r \in R} \phi_*(r\lambda_i x) = \sum_{i=1}^{n} \sum_{r \in R} \phi_*(r\mu_i x). \tag{8.13}$$

We claim that (8.13) implies that there are $\sigma \in S_n$ and $u_1, \ldots, u_n \in \mathcal{U}(R)$ such that $\lambda_{\sigma(i)} = u_i\mu_i$ for every $i = 1, \ldots, n$. We argue by induction. Actually the same argument is valid for the case $n = 1$ and the induction step. Every map $\alpha_{i,r} : x \mapsto \phi_*(r\lambda_i x)$ and every map $\beta_{i,r} : x \mapsto \phi_*(r\mu_i x)$ is an element of $\mathrm{Hom}(C_1, \mathcal{U}(\mathbb{C}))$. Thus, if $C_1^* = \{\psi_1, \ldots, \psi_k\}$ then we can express (8.13) as a linear combination of the ψ_{i_*} where the coefficient of ψ_{i*} in the right (left) side coincides with the number of $\alpha_{i,r}$ ($\beta_{i,r}$) equal to ψ_{i*}. Actually, $\psi_{1*}, \ldots, \psi_{k*}$ are linearly independent over $\mathbb{C}$, by Proposition 7.2.3, and hence the coefficients on both sides coincides. This implies that for every $i = 1, \ldots, n$ and $r \in R$ there is at least one $j = 1, \ldots, n$ and one $s \in R$ such that $\alpha_{i,r} = \beta_{j,s}$.

Consider the left R-module $\mathrm{Hom}(C_1, M_R)$ with the following equivalent relation

$$\lambda \sim \mu \Leftrightarrow \lambda = u\mu \text{ for some } u \in \mathcal{U}(R)$$

and the following reflexive and transitive relation

$$\lambda \preccurlyeq \mu \Leftrightarrow \lambda = r\mu \text{ for some } r \in R.$$

Then $\sim$ and $\preccurlyeq$ are compatible and hence $\preccurlyeq$ induces a reflexive and transitive relation in $X = \mathrm{Hom}(C_1, M_R)/\sim$. Lemma 8.2 implies that this relation is also antisymmetric, i.e. the induced order $\preccurlyeq$ in X is a partial order.

Thus among the $\sim$-classes of the maps $\lambda_1, \dots, \lambda_n, \mu_1, \dots, \mu_n$ there is one maximal element with respect to $\preccurlyeq$. Interchanging the roles of C_1 and C_2 (and replacing f by f^{-1}) and reordering the λ_i if needed we may assume that the class of λ_n is maximal. By the previous paragraph there is $j = 1, \dots, n$ and $s \in R$ such that $\alpha_{n,1} = \beta_{j,s}$. Reordering the μ_i's (which correspond to replacing f by its composition with the monomial transformation permuting the j-th and n-th coordinates), one may assume without loss of generality that $j = n$. Therefore $\phi(\lambda_n x) = \phi(s\mu_n x)$ for every $x \in C_1$. Therefore $\mathrm{Im}\,(\lambda_n - s\mu_n) \subseteq \ker \phi$. As $\mathrm{Im}\,(\lambda_n - s\mu_n)$ is a submodule of M_R and ϕ is a right generator of M^* we deduce that $\mathrm{Im}\,(\lambda_n - s\mu_n) = 0$, by Proposition 8.1, and hence $\lambda_n = s\mu_n$. Then $\lambda_n \preccurlyeq \mu_n$. By the maximality of the $\sim$-class of λ_n we deduce that $\lambda_n \sim \mu_n$, i.e. $\lambda_n = u_n\mu_n$ for some $u_n \in \mathcal{U}(R)$. In case $n = 1$ we have finished to prove the claim. For the induction step we have

$$\sum_{r\in R} \phi_*(r\lambda_n x) = \sum_{r\in R} \phi_*(ru_n\mu_n x) = \sum_{r\in R} \phi_*(r\mu_n x)$$

and subtracting this from (8.13) we obtain

$$\sum_{i=1}^{n-1}\sum_{r\in R} \phi_*(r\lambda_i x) = \sum_{i=1}^{n-1}\sum_{r\in R} \phi_*(r\mu_i x).$$

Then the claim follows by the induction hypothesis.

The claim then shows that for every $x = (x_1, \dots, x_n) \in C_1$ we have

$$f(x) = (\mu_1(x), \dots, \mu_n(x)) = (u_1\lambda_{\sigma(1)}(x), \dots, u_n\lambda_{\sigma(n)}(x)) = (u_1 x_{\sigma(1)}, \dots, u_n x_{\sigma(n)}),$$

that is f is the restriction to C_1 of the monomial transformation

$$T(x_1, \dots, x_n) = (u_1 x_{\sigma(1)}, \dots, u_n x_{\sigma(n)}).$$

(Observe that for every $u \in \mathcal{U}(R)$ the map $m \mapsto um$ is an element of $\mathrm{Aut}(M_R)$) □

If M is a finite right R-module and $r \in R$ then the map $\rho_r : M \to M$ given by $\rho_r(m) = mr$ is a group homomorphism. Using Proposition 7.1.2, for every $r \in R$, $m \in M$ and $\chi \in M^*$ we have

$$\begin{aligned}\Phi_M(mr)(\chi) &= (\Phi_M\rho_r(m))(\chi) = ((\rho_r^{**}\Phi_)(m))(\chi) = (\Phi_M(m)\rho_r^*)(\chi) = \rho_r^*(\chi)(m) = \chi\rho_r(m) = \chi(mr)\\ &= (r\chi)(m) = \Phi_M(m)(r\chi) = (\Phi_M(m)r)(\chi).\end{aligned}$$

Therefore $\Phi_M(mr) = \Phi_M(m)r$ for every $m \in M$ and every $r \in R$. In other words Φ_M is an isomorphism of R-modules.

8.4. Lemma *If M is a finite simple R-module then so is M^*. In particular, if M is a finite semisimple module then so is M^*.*

Proof. If M^* is not simple then there is a short exact sequence $0 \to N_1 \to M^* \to N_2 \to 0$ with $N_1 \neq 0$ and $N_2 \neq 0$. Then $0 \to N_2^* \to M^{**} \to N_1^* \to 0$ is a short exact sequence with $N_1^* \neq 0$ and N_2^*. Thus M^{**} is not simple. As $M \cong M^{**}$, M is not simple. □

8.5. Lemma *Let R be a finite ring and M a finite right R-module. Then*

$$(M/MJ(R))^* \cong (M^* : MJ(R)) = \mathrm{Soc}(M^*).$$

Proof. Applying the functor $-^*$ to the short exact sequence $0 \to MJ(R) \to M \to M/MJ(R) \to 0$ we obtain a short exact sequence $0 \to (M/MJ(R))^* \xrightarrow{f} M^* \to (MJ(R))^* \to 0$. As $M/MJ(R)$ is a $R/J(R)$-module and $R/J(R)$ is semisimple then so is $M/MJ(R)$ as R-module. Then $(M/MJ(R))^*$ is semisimple, by Lemma 8.4, and hence so is $(M/MJ(R))^* \cong f((M/MJ(R))^*) = (M^* : MJ(R))$. Thus $(M^* : MJ(R)) \subseteq \mathrm{Soc}(M^*)$. For the reverse inclusion observe that $J(R)\mathrm{Soc}(M^*) = 0$, as $\mathrm{Soc}(M^*)$ is semisimple. Thus, if $\chi \in \mathrm{Soc}(M^*)$, $m \in M$ and $r \in J(R)$ then $\chi(mr) = (r\chi)(m) = 0(m) = 0$. This shows that $\mathrm{Soc}(M^*) \subseteq (M^* : MJ(R))$. □

Let R be a finite ring and let S_1 and S_2 be two simple modules. Then every homomorphism $f : S_1 \to S_2$ is either 0 or an isomorphism, by the Schur's Lemma (Lemma 4.1). This implies that $S_1 \cong S_2$ if and only if $S_1^* \cong S_2^*$. Thus, if $S_1, \dots, S_k$ is a set of representatives of the right R-modules then $S_1^*, \dots, S_k^*$ is a set of representatives of the left R-modules. This implies that if $(R/J(R))_R \cong S_1^{n_1} \oplus \cdots \oplus S_k^{n_k}$ then ${}_RR/J(R) \cong S_1^{*n_1} \oplus \cdots \oplus S_k^{n_k *} \cong (R/J(R)_R)^*$. Therefore

$$ {}_RR/J(R) \cong (R/J(R)_R)^* \quad \text{and} \quad R/J(R)_R \cong ({}_RR/J(R))^*. \tag{8.14}$$

8.6. Proposition *Let R be a finite ring and let M be a finite R-module. Then the following conditions are equivalent.*

1. *$\mathrm{Soc}(M)$ is cyclic.*
2. *For every simple R-module S the multiplicity of S in $\mathrm{Soc}(M)$ is not greater than the multiplicity of S in $R/J(R)$.*
3. *M is isomorphic to a submodule of R^* (in the appropriate side).*

Proof. The equivalence of 1 and 2 is a consequence of Lemma 5.5.

3 implies 2. Suppose that M is isomorphic to a submodule of R_R^*. Then $\mathrm{Soc}(M)$ is isomorphic to a submodule of $\mathrm{Soc}(R_R^*)$ and hence $\mathrm{Soc}(M)$ is isomorphic to a submodule of $({}_RR/J(R))^* \cong R/J(R)$, by Lemma 8.5 and (8.14). Then 2 follows, by Lemma 4.2.1.

1 implies 3. Suppose that $\mathrm{Soc}(M)$ is cyclic (and suppose that M is a right R-module). Then $\mathrm{Soc}(M)$ is isomorphic to a submodule of $R/J(R)_R \cong ({}_RR/J(R))^* \cong \mathrm{Soc}(R^*)$, by Lemma 8.5 and (8.14). Then $\mathrm{Soc}(M)$ is isomorphic to a submodule of R^*. □

We are ready to obtain the characterization of the finite modules over finite rings that satisfies the EP.

8.7. Theorem [Woo09] *Let R be a finite module and let M be a finite module. Then the following conditions are equivalent.*

1. *The alphabet M has the EP.*
2. *M is pseudoinjective and $\mathrm{Soc}(M)$ is cyclic.*

Proof. We suppose that M is a right R-module.

2 implies 1. Suppose that M is pseudoinjective and $\mathrm{Soc}(M_R)$ is cyclic. By Proposition 8.6, one may assume that M is a submodule of R_R^*. Let C_1 and C_2 be linear codes of M^n and let $f : C_1 \to C_2$ be an isomorphism preserving the Hamming weight. As M is a submodule of R_R^*, we can see C_1 and C_2 as linear codes of $(R_R^*)^n$ and f as an isomorphism preserving the Hamming weight. As R^* is a Frobenius R-bimodule, by Theorem 8.3, R^* has the EP. Therefore there is $\sigma \in S_n$ and $u_1, \ldots, u_n \in \mathrm{Aut}(R_R^*)$ such that f extends to the following monomial transformation of $(R^*)_R^n$:

$$T(x_1, \ldots, x_n) = (u_1 x_{\sigma(1)}, \ldots, u_n x_{\sigma(n)}) \quad x_1, \ldots, x_n \in R^*.$$

Write $T = DP$ where $P(x_1, \ldots, x_n) = (x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ and $D(x_1, \ldots, x_n) = (u_1 x_1, \ldots, u_n x_n)$. Then P restricts to a monomial transformation mapping C_1 to a linear code C_3 of M^n. Let $C_{j,i}$ denote the projection of C_j into the i-th coordinate. Then $C_{j,i}$ is a linear code of length 1 over M and $x \mapsto u_i x$ defines an injective homomorphism $D_i : C_{3,i} \to C_{2,i}$ which preserves the Hamming weight. As M is pseudoinjective, the alphabet M has the EP for linear codes of length 1, by Proposition 6.9. Therefore, D_i extends to an automorphism τ_i of M. Then f is the restriction to C_1 of the following monomial transformation $F(x_1, \ldots, x_n) = (\tau_1 x_{\sigma(1)}, \ldots, \tau_n x_{\sigma(n)})$. This shows that the alphabet M has the EP.

1 implies 2. Conversely, suppose that the alphabet M has the EP. Then certainly M has the EP for length 1 and hence M is pseudoinjective by Proposition 6.9. It remains to show that $\mathrm{Soc}(M)$ is cyclic. We argue by contradiction, so suppose that $\mathrm{Soc}(M)$ is not cyclic. Then, by Lemma 5.5, there is a simple right R-module S such that the multiplicity of S in $\mathrm{Soc}(M)$ is greater than the multiplicity of S in $R/J(R)$. This implies that one of the Wedderburn components of $R/J(R)$ is of the form $A = M_m(F)$ for a field F and if S is the first column of $M_m(F)$, seen as R-module by extension of scalars via the projection $R \to R/J(R) \to M_m(F)$, then $\mathrm{Soc}(M)$ contains S^n for some $n > m$. We can identify $P = S^n$ with $M_{n,m}(F)$. In this way $P = M_{n,m}(F)$ is seen as a right A-module and then it is considered as a right R-module by restriction of scalars. By Example 3.2, and having in mind that $A \cong \mathrm{End}_F(F^m)$ and $P \cong \mathrm{Hom}_F(F^n, F^m)$, there is a positive integer N and codes linear codes $C_\pm$ of P^N together with an isomorphism $f : C_+ \to C_-$ of A-modules preserving the Hamming weight such that for one coordinate all the elements of C_+ have zero in that coordinate while this not happen for the elements of C_- with respect to any coordinate. Actually $\mathrm{Hom}_R(C_+, C_-) = \mathrm{Hom}_A(C_+, C_-)$ and hence we can see f as an isomorphism of R-modules. Morever, $P \subseteq \mathrm{Soc}(M) \subseteq M$ and we can then consider f as an isomorphism of linear codes of M^N preserving the Hamming weight, which certainly cannot be extended to a monomial transformation. This yields the desired contradiction. □

9. The extension property for ring alphabets

In this section we consider the special case when we consider a finite ring R as alphabet. The Frobenius property for R is going to be the key ingredient in this case.

Let R be a finite ring. As R and R^* have the same cardinality they are isomorphic as left (resp. right)-module, if and only if ${}_RR^*$ (resp. R_R^*) is cyclic. Actually both conditions are equivalent by the following lemma.

9.1. Lemma *Let $\chi \in R^*$. Then χ generates ${}_RR^*$ if and only if χ generates R_R^**

Proof. Suppose $R^* = R\chi$. Let I be a right ideal of R contained in $\ker \chi$. Then $I \subseteq \ker(r\chi)$ for every $r \in R$ and hence $I \subseteq \ker \phi$ for every $\phi \in R^*$. Thus $I = 0$, by Lemma 7.3. This proves that $\ker \chi$ does not contain any right ideal of R. Then χ generates R_R^*, by Proposition 8.1. □

Therefore we have

9.2. Proposition *The following conditions are equivalent for a finite ring R.*

1. *R is Frobenius as (R,R)-bimodule.*
2. *${}_RR \cong {}_RR^*$.*
3. *$R_R \cong R_R^*$.*

We say that R is a *Frobenius ring* if it is Frobenius as (R,R)-bimodule.

9.3. Theorem *Let R be a finite ring. Then the following conditions are equivalent.*

1. *R is a Frobenius ring.*
2. *The alphabet R_R has the EP.*
3. *The alphabet ${}_RR$ has the EP.*

Proof. By symmetry (and Proposition 9.2) it is enough to show that $R_R \cong R_R^*$ if and only if R_R has the EP. By Theorem 8.3, R_R^* has the EP and therefore if $R_R \cong R_R^*$ then R_R has also the EP. Conversely, suppose that R_R has the EP. Then $\mathrm{Soc}(R)$ is cyclic by Theorem 8.7 and hence R_R is isomorphic to a submodule of R_R^* by Proposition 8.6. Since R and R^* have the same cardinality we deduce that $R \cong R_R^*$. □

We close this section with other alternative characterizations of finite Frobenius rings which will be useful in the subsequent sections.

9.4. Theorem [Hon01] *The following conditions are equivalent for a finite ring:*

1. *R is Frobenius.*
2. *$\mathrm{Soc}(R_R) \cong (R/J(R))_R$.*
3. *$\mathrm{Soc}({}_RR) \cong {}_R(R/J(R))$.*

The Goldie dimension of a module M is the maximum positive integer n such that there is a family with n independent non-zero submodules of M. Let $\mathrm{GD}(M)$ denote the Goldie dimension of M. Clearly, if N is a submodule of M then $\mathrm{GD}(N) \leq \mathrm{GD}(M)$. Using Proposition 4.2 it is easy to see that if M is the direct sum of n simple modules then $\mathrm{GD}(M) = n$.

If M is finite module then $\mathrm{GD}(\mathrm{Soc}(M)) = \mathrm{GD}(M)$. Indeed, if $\{N_i : i \in I\}$ is an independent family of non-zero submodules of M then $\mathrm{Soc}(N_i) \neq 0$ for every i (because N_i is finite) and obviously $\{\mathrm{Soc}(N_i) : i \in I\}$ is an independent family of non-zero submodules of M. Therefore $\mathrm{GD}(M) \leq \mathrm{GD}(\mathrm{Soc}(M))$. Thus $\mathrm{GD}(M) = \mathrm{GD}(\mathrm{Soc}(M))$.

Let R be a ring. An element $e \in R$ satisfying $e = e^2$ is said to be *idempotent*. Two elements $x, y \in R$ with $xy = yx = 0$ are said to be *orthogonal*. Observe that if $e_1, \ldots, e_n$ are orthogonal idempotents of R then $\{Re_1, \ldots, Re_n\}$ is independent. Indeed, if $x \in Re_1 \cap \bigcap_{j=2}^n Re_i$. Then $x = xe_1 = x_2e_2 + \cdots + x_ne_n$. Then $x = xe_1 = x_2e_2e_1 + \cdots + x_ne_ne_1 = 0$.

9.5. Lemma *Let R be a finite ring and let $E_1, \ldots, E_n$ mutually orthogonal idempotents of $R/J(R)$ with $E_1 + \cdots + E_n = 1$. Then there are mutually orthogonal idempotents $e_1, \ldots, e_n$ in R with $1 = e_1 + \cdots + e_n$ and $E_i = e_i + J(R)$ for every i.*

Proof. This is a consequence of the fact that $R/J(R)$ is semisimple and $J(R)^n = 0$ for some n. For the details see Proposition 27.1, Proposition 27.4 and Theorem 27.6 in [AF92]. □

9.6. Lemma *If R is a finite ring then $\mathrm{GD}(R_R) = \mathrm{GD}(\mathrm{Soc}(R_R)) \geq \mathrm{GD}((R/J(R)_R)$.*

Proof. Let $R/J(R) = S_1 \oplus \cdots \oplus S_n$ with each S_i a simple module. Then $\mathrm{GD}(R/J(R))) = n$. By (2.3) and the isomorphism $R/J(R) \cong \mathrm{End}(R/J(R))$ there are non-zero orthogonal idempotents $E_1, \ldots, E_n$ in $R/J(R)$ with $1 = E_1 + \cdots + E_n$ (take in the matrix form the idempotents having 1 in one diagonal entry and zero in all the other entries). By Lemma 9.5, there are non-zero orthogonal idempotents $e_1, \ldots, e_n$ in R. Then $\mathrm{GD}(R) \geq n$. □

9.7. Proposition [DLP04] *Let R be a finite ring. Then R is Frobenius if and only if $\mathrm{Soc}(R_R)$ is cyclic if and only if $\mathrm{Soc}({}_RR)$ is cyclic.*

Proof. Suppose $S_1, \ldots, S_k$ are representatives of the simple right R-modules and that $R/J(R) \cong S_1^{n_1} \oplus \cdots \oplus S_k^{n_k}$ and $\mathrm{Soc}(R_R) \cong S_1^{m_1} \oplus \cdots \oplus S_k^{m_k}$. Then $\sum_{i=1}^k m_k = \mathrm{GD}(\mathrm{Soc}(R)) = \mathrm{GD}(R) \geq \mathrm{GD}(R/J(R)) = n_1 + \cdots + n_k$. If R is Frobenius then $\mathrm{Soc}(R_R) \cong R/J(R)$, by Theorem 9.4, hence $\mathrm{Soc}(R_R)$ is cyclic. Conversely, if $\mathrm{Soc}(R_R)$ is cyclic then, by Proposition 8.6, $m_i \leq n_i$ for every i. Then necessarily $m_i = n_i$ for every i and hence $\mathrm{Soc}(R_R) \cong (R/J(R))_R$. Then R is Frobenius by Theorem 9.4. □

10. The MacWiliams Identities for group alphabets

In order to have MacWilliams identities for module alphabets we need a notion of dual which satisfies properties alike the following ones holding for linear codes C and D with alphabet a finite field F:

(D1) If $C \subseteq D$ then $D^\perp \subseteq C^\perp$.

(D2) $C^{\perp\perp} = C$.
(D3) $|C|\,|C^{\perp}| = |F|^n$.
(D4) $W_{C^{\perp}}(X,Y) = \frac{1}{|C|} W_C(X + (|F|-1)Y, X - Y)$.

The notion of weight enumerator can be extended to arbitrary abelian groups and in particular to modules. More precisely, if A is an abelian group and C is a subgroup of A^n (i.e. a $\mathbb{Z}$-submodule) then the *weight enumerator* of C is the following polynomial in two variables:

$$W_C(X,Y) = \sum_{c\in C} X^{n-w(c)}Y^{w(c)} = \sum_{i=0}^{n} A_{C,i}X^{n-i}Y^{j},$$

where $A_{C,i}$ denotes the number of codewords of C of weight i.

Our aim now is to obtain some notion of dual code for linear codes over module alphabets satisfying properties similar to (D1)-(D4). For the moment we are going to consider only abelian groups.

Let A be a finite abelian group. For every vector space V over $\mathbb{C}$ let V^A denote the set of maps $A \to V$. We endow V^A with structure of vector space over $\mathbb{C}$, by setting

$$(f+g)(a) = f(a) + g(a) \quad \text{and} \quad (\alpha f)(x) = \alpha f(x) \quad (f, g \in V^A, a \in A, \alpha \in \mathbb{C}).$$

The *Fourier transform* of $f \in V^A$ is the map $\widehat{f} \in V^{A^*}$ defined by

$$\widehat{f}(\chi) = \sum_{a\in A} \chi_*(a) f(a) \quad (\chi \in A^*).$$

10.1. Proposition [Fourier Inversion Formula] *If A is a finite abelian group, $a \in A$ and $f \in V^A$ then*

$$f(a) = \frac{1}{|A|} \sum_{\chi\in A^*} \chi_*(-a)\widehat{f}(\chi).$$

Proof. By Proposition 7.1 we have

$$\sum_{\chi\in A^*} \chi_*(-a)\widehat{f}(\chi) = \sum_{\chi\in A^*} \chi_*(-a) \sum_{b\in A} \chi_*(b) f(b) = \sum_{b\in A} \left(\sum_{\chi\in A^*} \chi_*(b-a) \right) f(b) = |A| f(a)$$

□

10.2. Theorem [Poisson Summation Formula] *Let H be a subgroup of a finite abelian group A and let V be a vector space over $\mathbb{C}$. Then for every $a \in A$ and $f \in V^A$ we have*

$$\sum_{h\in H} f(a+h) = \frac{1}{[A:H]} \sum_{\chi\in(A^*:H)} \chi_*(-a)\widehat{f}(\chi).$$

In particular, for $a = 0$ we have

$$\sum_{h\in H} f(h) = \frac{1}{[A:H]} \sum_{\chi\in(A^*:H)} \widehat{f}(\chi).$$

Proof. By Proposition 7.2.1,

$$\sum_{h\in H} \chi(h) = \begin{cases} |H|, & \text{if } \chi \in (A^* : H); \\ 0, & \text{if } \chi \in A^* \setminus (A^* : H). \end{cases}$$

Combining this with the Fourier Inversion Formula (Proposition 10.1) we have

$$\sum_{h\in H} f(a+h) = \frac{1}{|A|} \sum_{\chi\in A^*} \chi_*(-a)\widehat{f}(\chi) \sum_{h\in H} \chi_*(-h) = \frac{|H|}{|A|} \sum_{\chi\in(A^*:H)} \chi_*(-a)\widehat{f}(\chi) = \frac{1}{[A:H]} \sum_{\chi\in(A^*:H)} \chi_*(-a)\widehat{f}(\chi).$$

□

Consider the complex algebra $\mathbb{C}[X,Y]$ of polynomials in two variables X and Y with coefficients in $\mathbb{C}$, and consider the map $f : A \to \mathbb{C}[X,Y]$ given by

$$f(a) = X^{1-w(a_i)}Y^{w(a_i)}.$$

For every $\chi \in A^*$, we have

$$\widehat{f}(\chi) = \sum_{a\in A} \chi_*(a) f(a) = \sum_{a\in A} \chi_*(a) X^{1-w(a)}Y^{w(a)} = \chi(0)X + Y \sum_{a\in A\setminus\{0\}} \chi(a) = X - Y + Y \sum_{a\in A} \chi(a)$$

Therefore, using Proposition 7.2.1, we have

$$\widehat{f}(\chi) = \begin{cases} X - (|A|-1)Y, & \text{if } \chi = 0; \\ X - Y, & \text{otherwise.} \end{cases} \tag{10.15}$$

Let us keep denoting as f the map $A^n \to \mathbb{C}[X,Y]$ given by

$$f(a_1,\dots,a_n) = \prod_{i=1}^n f(a_i) = \prod_{i=1}^n X^{1-a_i}Y^{a_i}.$$

By (2.2) we have $(A^n)^* \cong (A^*)^n$. We consider this isomorphism as an equality. Then we can consider each $\chi = (\chi_1,\dots,\chi_n) \in (A^*)^n$ as an element of $(A^n)^*$ and we have

$$\widehat{f}(\chi) = \widehat{f}(\chi_1,\dots,\chi_n) = \sum_{(a_1,\dots,a_n)\in A^n} \prod_{i=1}^n \chi_{i*}(a_i)f(a_i) = \prod_{i=1}^n \sum_{a_i\in A} \chi_{i*}(a_i)f(a_i) = \prod_{i=1}^n \widehat{f}(\chi_i). \tag{10.16}$$

Combining (10.15) and (10.16) we deduce

$$\widehat{f}(\chi) = (X + (|A|-1)Y)^{n-w(\chi)}(X-Y)^{w(\chi)}. \tag{10.17}$$

If C is a linear code of A^n (i.e. a subgroup of A) then $C^\perp = ((A^n)^* : C)$ is a subgroup of $(A^n)^*$. Using (2.2) to identify $(A^n)^*$ and $(A^*)^n$, we can see $C^\perp$ as a linear code of $(A^*)^n$ (i.e. a subgroup of $(A^*)^n$). On the other hand, identifying $(A^n)^{**}$ with A^n we can define $D^\perp = (A^n : D)$ for D a subgroup of $(A^n)^*$. Clearly $D^\perp$ is a subgroup of A^n and $C \subseteq C^{\perp\perp}$. Furthermore $C^\perp \cong (A^n/C)^*$ and therefore $|C|\,|C^\perp| = |A|^n$. Thus $|C| = |C^{\perp\perp}|$ and thus $C = C^{\perp\perp}$. This proves the first three statements of the following Theorem.

10.3. Theorem *Let A be a finite abelian group and let C be a subgroup of A^n. Then*

1. *$C^\perp$ is a subgroup of A^*.*
2. *$C^{\perp\perp} = C$.*
3. *$|C|\,|C^\perp| = |A|^n$.*
4. *$W_{C^\perp}(X,Y) = \frac{1}{|C|}W_C(X + (|A|-1)Y, X-Y)$ [MacWilliams Identities].*

Proof. The first equality in the next calculations is just the definition of the weight enumerator, the second one follows from the Poisson Inversion Formula (Theorem 10.2) and the third one follows from (10.17):

$$\begin{aligned} W_C(X,Y) &= \sum_{x\in C} f(x) = \frac{1}{[A^n:C]} \sum_{\chi\in((A^n)^*:C)} \widehat{f}(\chi) = \frac{1}{|C^\perp|}\sum_{\chi\in C^\perp} (X+(|A|-1)Y)^{n-w(\chi)}(X-Y)^{w(\chi)} \\ &= \frac{1}{|C^\perp|}W_{C^\perp}(X+(|A|-1)Y, X-Y). \end{aligned}$$

Then statement 4 follows interchanging the roles of C and $C^\perp$. □

Theorem 10.3 is very similar to the goal we addressed at the beginning of this section, except that C and $C^\perp$ live in a different ambient spaces. To avoid this we introduce the following notion.

A *biadditive map* is a map $\beta : A \times B \to C$, where A, B and C are abelian (additive) groups, satisfying

$$\beta(a+a',b) = \beta(a,b) + \beta(a',b) \quad \text{and} \quad \beta(a,b+b') = \beta(a,b) + \beta(a,b') \quad (a,a',\in A, b,b'\in B).$$

In that case we have group homomorphisms

$$A \xrightarrow{\beta_l} \mathrm{Hom}_{\mathbb{Z}}(B,C) \quad \text{and} \quad B \xrightarrow{\beta_r} \mathrm{Hom}_{\mathbb{Z}}(A,E)$$

with

$$\beta_l(a)(b) = \beta_r(b)(a) = \beta(a,b) \quad (a\in A, b\in B).$$

Moreover, if n is a positive integer then β induces a biadditive map

$$\beta : A^n \times B^n \to C$$

with

$$\beta((a_1,\dots,a_n),(b_1,\dots,b_n)) = \beta(a_1,b_1) + \cdots + \beta(a_n,b_n).$$

Let β be a biadditive map. Then β is said to be *non-degenerate* if both β_l and β_r are injective.

Suppose that A and B are finite groups and that $\beta : A \times B \to \mathbb{Q}/\mathbb{Z}$ is a non-degenerate additive map. Then $\beta_l : A \to B^*$ and $\beta_r : B \to A^*$ are injective and therefore

$$|A| \le |B^*| = |B| \le |A^*| = |A|$$

by Proposition 7.1. Therefore $|A| = |B| = |A^*| = |B^*|$ and hence β_l and β_r are isomorphisms. Thus $A \cong B^* \cong B$.

Clearly the extension of β to a biadditive map β in $A^n \times B^n$ is also non-degenerate and therefore it induces isomorphisms $\beta_l, \beta_r : A^n \to (B^n)^* \cong (B^*)^n$. If C is a subgroup of A^n then we define the *right annihilator*

$$\mathrm{r}(C) = \beta_r^{-1}(C^\perp) = \{b \in B^n : \beta(C,b) = 0\}$$

and for a subgroup D of B^n we define the *left annihiliator*

$$\mathrm{l}(C) = \beta_l^{-1}(D^\perp) = \{a \in A^n : \beta(a,D) = 0\}.$$

Applying Theorem 10.3 we obtain

10.4. Corollary *Let A and B be finite abelian groups and let $\beta : A \times B \to \mathbb{Q}/\mathbb{Z}$ be a non-degenerate biadditive map. Then the left and right annihilators* l *and* r *in A^n satisfy the following properties for every subgroup C of A^n and every subgroup D of B^n:*

1. *$\mathrm{r}(C)$ is a subgroup of B^n and $\mathrm{l}(D)$ is a subgroup of A^n.*
2. *$\mathrm{l}(\mathrm{r}(C)) = C$ and $\mathrm{r}(\mathrm{l}(D)) = D$.*
3. *$|C|\,|\mathrm{r}(C)| = |D|\,|\mathrm{r}(D)| = |A|^n = |B|^n$.*
4. *$W_{\mathrm{r}(C)} = \frac{1}{|C|}W_C(X + (|A| - 1)Y, X - Y)$ and $W_{\mathrm{l}(D)} = \frac{1}{|D|}W_C(X + (|B| - 1)Y, X - Y)$.*

A biadditive map $\beta : A \times A \to E$ is said to be *symmetric* if $\beta(a, b) = \beta(b, a)$ for every $a, b \in A$. Clearly the left and right annihilators coincides for symmetric bilinear forms. Corollary 10.4 implies that if $\beta : A \times A \to \mathbb{Q}/\mathbb{Z}$ is a symmetric non-degenerate biadditive map then using the annihilators to define dual codes, conditions (D1)-(D4) hold. Next proposition ensures the existence of such biadditive map for every finite abelian group.

10.5. Proposition *Every finite abelian group A admits a non-degenerate symmetric biadditive map $A \times A \to \mathbb{Q}/\mathbb{Z}$.*

Proof. To prove this we observe that

$$\begin{array}{ccc} \beta : A \times A^* & \to & \mathbb{Q}/\mathbb{Z} \\ (x, \chi) & \mapsto & \chi(x) \end{array}$$

defines a non-degenerate biadditive map. By Proposition 7.1.1, there is an isomorphism $\lambda : A \to A^*$ satisfying $\lambda(a)(b) = \lambda(b)(a)$ for every $a, b \in A$. Then $\beta'(a, b) = \beta(a, \lambda(b))$ defines a non-degenerate symmetric biadditive map $A \times A \to \mathbb{Q}/\mathbb{Z}$. □

11. MacWilliams identities for module alphabets

We now address the question of finding a notion of dual in module alphabets. In the previous section we have seen how biadditive maps helps to define a notion of dual on group alphabets. The classical biadditive map used to define dual codes of linear codes over field alphabets is the product in F which when extended to a biadditive map in F^n gives the standard dot product:

$$\begin{array}{ccc} F^n \times F^n & \to & F \\ ((a_1, \ldots, a_n), (b_1, \ldots, b_n)) & \mapsto & a_1b_1 + \cdots + a_nb_n. \end{array}$$

If F is replaced by an arbitrary ring R then the dot product is not symmetric anymore and if C is a submodule of ${}_RR^n$ then $\mathrm{r}(C)$ is a submodule of R_n^n. Similarly, if D is a submodule of R_R^n then $\mathrm{l}(D)$ is a submodule of ${}_RR^n$. Therefore, it is natural to expect that the dual operator should associate right linear codes to left linear codes and vice versa. Thus the conditions (D1)-(D4) should vary slightly. We start translating the notion of biadditive map to this context.

Let R and S be rings, let ${}_RP$ be a left R-module, Q_S a right S-module and ${}_RE_S$ an (R, S)-bimodule. A map $\beta : P \times Q \to E$ is said to be *bilinear* if it is biadditive and satisfies the following condition

$$\beta(rp, q) = r\beta(p, q) \quad \text{and} \quad \beta(p, qs) = \beta(p, q)s, \quad (r \in R, p \in P, q \in Q, s \in S).$$

Equivalently, β is bilinear if and only if for every $p \in P$ the map

$$\begin{array}{ccc} Q & \xrightarrow{\beta_{\mathrm{l}(p)}} & E \\ q & \mapsto & \beta(p, q) \end{array}$$

is a homomorphism of right S-modules and for every $q \in Q$ the map

$$\begin{array}{ccc} P & \xrightarrow{\beta_{\mathrm{r}(q)}} & E \\ p & \mapsto & \beta(p, q) \end{array}$$

is a homomorphism of left R-modules. Other equivalent versions are $\beta_l : P \to \mathrm{Hom}(Q_S, E_S)$ is a homomorphism of left R-modules, or equivalently $\beta_r : Q \to \mathrm{Hom}({}_RP, {}_RE)$ is a homomorphism of right S-modules.

If $\beta : P \times Q \to E$ is a bilinear map and n is a positive integer then the extension $\beta : P^n \times Q^n \to E$ is also bilinear. If C is a submodule of P^n then the *right annihilator*

$$\mathrm{r}(C) = \{q \in Q^n : \beta(C, q) = 0\}$$

is a submodule of Q^n. Similarly, if D is a submodule of Q^n then the *left annihilator*

$$\mathrm{l}(D) = \{p \in P^n : \beta(p, D) = 0\}$$

is a submodule of P^n. Moreover the following properties holds for all submodules C and C' of P^n and all submodules D and D' of Q^n.

1. If $C \leq C'$ then $\mathrm{r}(C') \subseteq \mathrm{r}(C)$.
2. If $D \leq D'$ then $\mathrm{r}(D') \subseteq \mathrm{r}(D)$.
3. $C \subseteq \mathrm{l}(\mathrm{r}(C))$ and $D \subseteq \mathrm{r}(\mathrm{l}(D))$.

11.1. Theorem [Woo09] *Let R and S be finite rings, P a finite left R-module, Q a finite right S module and E a finite (R,S)-bimodule. Let $\beta : P \times Q \to E$ be a non-degenerate bilinear map and suppose that there is $\chi \in E^*$ such that $\ker \chi$ does not contain non-zero submodules of neither ${}_RE$ nor E_S. Let $\beta' = \chi \circ \beta$. Let l' and r' be the left and annihilator maps associated to β'. Then the following properties hold:*

1. *β' is a non-degenerate biadditive map.*
2. *For every positive integer n and every submodule C of P^n we have $\mathrm{r}(C) = \mathrm{r}'(C)$, $\mathrm{l}(\mathrm{r}(C)) = C$, $|C|\,|\mathrm{r}(C)| = |P|^n$ and $W_{\mathrm{r}(C)}(X,Y) = \frac{1}{|C|} W_C(X + (|P|-1)Y, X - Y)$.*
3. *For every positive integer n and every submodule D of Q^n we have $\mathrm{l}(D) = \mathrm{l}'(C)$, $\mathrm{r}(\mathrm{l}(D)) = D$, $|D|\,|\mathrm{l}(D)| = |Q|^n$ and $W_{\mathrm{l}(D)}(X,Y) = \frac{1}{|D|} W_C(X + (|Q|-1)Y, X - Y)$.*

Proof. (1) Obviously β' is biadditive. Let $q \in Q$ with $\beta'(P,q) = 0$. Then the map $\beta_l(q) : P \to E$ is a homomorphism of left R-modules and hence $\mathrm{Im}\ \beta_l(q)$ is a submodule of ${}_RE$ contained in the kernel of χ. By assumption, $\mathrm{Im}\ \beta_l(q) = 0$ and therefore $\beta(P,q) = 0$. As β is non-degenerate we have $q = 0$. Similarly, if $\beta'(p,Q)$ for some $p \in P$ we have $p = 0$. This proves that β' is non-degenerate.

2 and 3. Let C be a submodule of P^n. Obviously $\mathrm{r}(C) \subseteq \mathrm{r}'(C)$. Let $b \in \mathrm{r}'(C)$. Then $\beta(C,b) = \beta_l(b)(C)$ is a submodule of ${}_RE$ contained in $\ker \chi$. Therefore $\beta(C,b) = 0$ and hence $b \in \mathrm{r}(C)$. Then $\mathrm{r}(C) = \mathrm{r}'(C)$. Similarly $\mathrm{l}(D) = \mathrm{l}'(D)$ for every submodule D of Q^n. The rest of the properties follow from Corollary 10.4. □

12. MacWilliams identities for ring alphabets

An important example of non-degenerate bilinear map is the multiplication map

$$\begin{array}{ccc} R \times R & \to & R \\ (r,s) & \mapsto & rs \end{array}$$

for R any arbitrary ring. We will refer to this as the *standard bilinear map* of R. Its right annihilator operator r maps left ideals of R to right ideals of R and its left annihilator operator l maps right ideals of R to left ideals of R. If we want that l and r could serve to define a notion of dual for linear codes in the alphabet R, l and r must be mutually inverse operators, in other words they should satisfy the following condition: We say that a ring R satisfies the *double annihilator condition* if it satisfies

$$\mathrm{l}(\mathrm{r}(I)) = I, \qquad \text{for every left ideal } I \text{ of } R \tag{12.18}$$

$$\mathrm{r}(\mathrm{l}(J)) = J, \qquad \text{for every right ideal } J \text{ of } R. \tag{12.19}$$

12.1. Theorem *Let R be a finite ring. Then the following conditions are equivalent:*

1. *R satisfies the double annihilator condition.*
2. *R_R is injective.*
3. *${}_RR$ is injective.*

Proof. We prove that 1 and 2 are equivalent. By symmetry, 1 and 3 are also equivalent.

First of all observe that

$$\mathrm{l}(I_1 + I_2) = \mathrm{l}(I_1) \cap \mathrm{l}(I_2) \quad \text{and} \quad \mathrm{r}(J_1 + J_2) = \mathrm{r}(J_1) \cap \mathrm{r}(J_2) \tag{12.20}$$

for every left ideals I_1 and I_2 and right ideals J_1 and J_2.

1 implies 2. Suppose that R satisfies the double annihilator condition. If J_1 and J_2 are right ideals of R then, by (12.20) we have $\mathrm{l}(J_1 \cap J_2) = \mathrm{l}(\mathrm{r}(\mathrm{l}(J_1)) \cap r(\mathrm{l}(J_2))) = \mathrm{l}(\mathrm{r}(\mathrm{l}(J_1) + \mathrm{l}(J_2))) = \mathrm{l}(J_1) + \mathrm{l}(J_2)$. Similarly, if I_1 and I_2 are left ideals of R then $\mathrm{r}(I_1 \cap I_2) = \mathrm{r}(I_1) + \mathrm{r}(I_2)$.

To see that R_R is injective we apply Baer Criterion (Theorem 6.3). Let J be a right ideal of R and let $f : J \to R$ be a homomorphism of right R-modules. As R is finite there are $r_1, \ldots, r_k \in J$ such that $J = r_1R + \cdots + r_kR$. We have to show that there is $a \in R$ such that $f(x) = ax$ for every $x \in J$. We argue by induction on k. Suppose first that $k = 1$ and let $s = f(r_1)$. Then $sx = f(r_1x)$ for every $x \in R$ and therefore $s\,\mathrm{r}(Rr_1) = 0$. In other words $s \in \mathrm{l}(\mathrm{r}(Rr_1)) = Rr_1$ and hence $s = ar_1$ for some $a \in R$. Therefore $f(r_1x) = sx = ar_1x$ for every $x \in R$. Thus $f(x) = ax$ for every $x \in J$, as desired. Suppose that $k > 1$ and let $J_1 = r_2R + \cdots + r_{k-1}R$. By the case $k = 1$ there is $a_1 \in R$ such that $f(x) = a_1x$ for every $x \in r_1R$. Moreover, by induction hypothesis there is $a_2 \in R$ such that $f(x) = a_2x$ for every $x \in J_1$. Then $a_1 - a_2 \in \mathrm{l}(r_1R \cap J_1) = \mathrm{l}(r_1R) + \mathrm{l}(J_1)$. Write $a_1 - a_2 = a_1' - a_2'$ with $a_1' \in \mathrm{l}(r_1R)$ and $a_2' \in \mathrm{l}(J_1)$ and let $a = a_1 - a_1' = a_2 - a_2'$. Let $x \in J$. Thus $x = x_1 + x_2$ with $x_1 \in r_1R$ and $x_2 \in J_1$. Then $f(x) = f(x_1) + f(x_2) = a_1x_1 + a_2x_2 = (a + a_1')x_1 + (a + a_2')x_2 = a(x_1 + x_2) = ax$.

2 implies 1. Suppose that R_R is injective.

Claim 1: $\mathrm{l}(J_1 \cap J_2) = \mathrm{l}(J_1) + \mathrm{l}(J_2)$ for all right ideals J_1 and J_2 of R.

Indeed, the inclusion $\mathrm{l}(J_1)+\mathrm{l}(J_2)\subseteq \mathrm{l}(J_1\cap J_2)$ is clear. Conversely, let $x\in \mathrm{l}(J_1\cap J_2)$. Then the map $f(a_1+a_2)=xa_2$, for $a_1\in J_1$ and $a_2\in J_2$, is a well defined homomorphism $f: J_1+J_2\mapsto R$. As R_R is injective there is $y\in R$ such that $xa_2=y(a_1+a_2)$ for every $a_1\in J_1$ and $a_2\in J_2$. In particular, $ya_1=0$ for every $a_1\in J_1$ and $xa_2=ya_2$ for every $a_2\in J_2$ and hence $y\in \mathrm{l}(J_1)$ and $x-y\in \mathrm{l}(J_2)$, so that $x\in \mathrm{l}(J_1)+\mathrm{l}(J_2)$. This finishes the proof of Claim 1.

Claim 2: R satisfies (12.18).

Suppose first that $I=Rr$ for some $r\in R$ and let $s\in \mathrm{l}(\mathrm{r}(I))$. Let $f: I\to R$ be the map defined by $f(rx)=sx$. This is well defined because if $rx=0$ then $x\in \mathrm{l}(I)$ and hence $sx=0$. By hypothesis, there is $a\in R$ such that $sx=f(rx)=arx$ for every $x\in R$. Applying this for $x=1$ we deduce that $s=ar\in I$. Thus $\mathrm{l}(\mathrm{r}(I))=I$, as desired.

Now let I an arbitrary left ideal of R. As R is finite, $I=\sum_{i=1}^n Rr_i$ for some $r_i\in R$ then, using (12.20) and Claim 1 we have

$$\mathrm{l}(\mathrm{r}(I))=\mathrm{l}\left(\mathrm{r}\left(\sum_{i=1}^n Rr_i\right)\right)=\mathrm{l}\left(\bigcap_{i=1}^n \mathrm{r}(Rr_i)\right)=\sum_{i=1}^n \mathrm{l}(\mathrm{r}(Rr_i))=\sum_{i=1}^n Rr_i=I.$$

This finishes the proof of Claim 2.

Claim 3: Every simple left R-module is isomorphic to a left ideal of R.

Let S be a simple left R-module. Fix $0\neq s\in S$ and let $I=\{r\in R: rs=0\}$. Then I is the kernel of the map $R\to S$ given by $r\mapsto rs$. As $S=Rs$, because S is simple, this map is surjective and therefore $g(r+I)=rs$ defines an isomorphism $g: R/I\to S$. By Claim 2, $\mathrm{l}(\mathrm{r}(I))=I\neq R=\mathrm{l}(0)$ and hence $\mathrm{r}(I)\neq 0$. Let $0\neq r\in \mathrm{r}(I)$. Using again that S is simple we deduce that $S\cong h(S)$, so that S is isomorphic to a left ideal of R. This finishes the proof of Claim 3.

Claim 4: Every simple right R-module is isomorphic to a right ideal of R.

Let $S_1,\dots,S_n$ be representatives up to isomorphisms of the simple left modules. For every $i=1,\dots,n$, let P_i be the sum of the left ideals of R isomorphic to S_i and

$$B_i=P_i\cap \mathrm{l}(J(R)).$$

Then $\mathrm{Soc}({}_RR)=P_1\oplus\cdots\oplus P_n$ and P_i and B_i are a two-sided ideal of R for every i. Moreover, by Claim 3, $P_i\neq 0$ for every $i=1,\dots,n$. By Lemma 5.6, if $P_iJ(R)^k\neq 0$ then $P_iJ(R)^k\neq P_iJ(R)^{k+1}$. As R is finite we deduce that there is $k\geq 0$ such that $P_iJ(R)^k\neq 0$ and $P_iJ(R)^{k+1}=0$. Then $0\neq P_iJ(R)^k\subseteq B_i$. Thus $B_i\neq 0$. As $B_iJ(R)=0$, we deduce that B_i is a non-zero semisimple right R-module and hence it contains a minimal right ideal T_i. We claim that if $T_i\cong T_j$ then $i=j$. Indeed, let $f: T_i\to T_j$ be an isomorphism of right R-modules. As R_R is injective, there is $r\in R$ such that $f(x)=rx$ for every $x\in T_i$. Then $T_j\subseteq P_j\cap rP_i\subseteq P_j\cap P_i=0$, a contradiction. Therefore R_R contains at least n non-isomorphic simple right R-modules. As the number of simple right R-modules coincides with the number of simple left R-modules, and this number is n we deduce that every simple right R-module is isomorphic to a right ideal of R. This finishes the proof of Claim 4.

Claim 5: If M is a non-zero right R-module then $\mathrm{Hom}(M,R_R)\neq 0$.

By Lemma 5.6, $M\neq MJ(R)$. Hence $M/MJ(R)$ is a non-zero semisimple right R-module. Thus there is a non-zero homomorphism $M\to S$ for some simple right R-module. By Claim 4, S is isomorphic to a left ideal of R and hence there is a non-zero homomorphism $M\to R$. This finishes the proof of Claim 5.

We are ready to finish the proof by showing that R satisfies (12.19). Let J be a right ideal of R and let $M=\mathrm{r}(\mathrm{l}(J))/J$. Let $f\in \mathrm{Hom}(M,R_R)$. Composing f with the natural homomorphism $\mathrm{r}(\mathrm{l}(J))\mapsto \mathrm{r}(\mathrm{l}(J))/J$ we have a homomorphism $\mathrm{r}(\mathrm{l}(J))\to R$ vanishing on J. Since R_R is injective there is $r\in R$ such that $f(x+J)=rx$ for every x. Then $r\in \mathrm{l}(J)$ and hence $f(r)=rx=0$ for every $x\in \mathrm{r}(\mathrm{l}(J))$. In other words $f=0$. This shows that $\mathrm{Hom}(M,R_R)=0$ and therefore $M=0$, by Claim 5. Thus $\mathrm{r}(\mathrm{l}(J))=J$, as desired. □

Observe that every Frobenius finite ring satisfy the double annihilator condition because $R_R\cong R_R^*$ and R^*R is injective by Proposition 6.8.

12.2. Theorem [Woo09] *Let R be a finite ring. If R is satisfies the double annihilator condition but it is not Frobenius then R has a left ideal I such that $|I|\,|\mathrm{r}(I)|<|R|$ and a right ideal J such that $|J|\,|\mathrm{l}(J)|<|R|$.*

Proof. Suppose that R satisfies the double annihilator condition but it is not Frobenius. By Proposition 9.7, $\mathrm{Soc}({}_RR)$ is not cyclic and hence, by Proposition 8.6, there is a simple left R-module I such that the multiplicity n of I on $\mathrm{Soc}({}_RR)$ is greater that the multiplicity of I in $R/J(R)$. As $\mathrm{Soc}({}_RR)$ contains a submodule isomorphic to I, we may assume without loss of generality that I is a left ideal of R. As I is simple $I=Rx$ for every $0\neq x\in I$. Let $\lambda_x: R\to R$ be given by $\lambda_x(r)=xr$. Then $\mathrm{r}(I)=\ker\lambda_x\cong R/\mathrm{Im}\ \lambda_x=R/xR$. Therefore $|I|\,|\mathrm{r}(I)|=\frac{|Rx|}{|xR|}|R|$.

By the description of the simple left modules of R, I can be seen as a column of a matrix ring $M_m(F)$ for some field F such that $M_m(F)$ is one of the Wedderburn components of $R/J(R)$. Then the multiplicity of I on $R/J(R)$ is $m<n$. Then I is considered as an R-module by restrictions of scalars via the natural

homomorphism $R \to R/J(R)$ and the projection $R/J(R) \to M_n(F)$. Then I^m can be seen as $M_{m,n}(F)$ as a left $M_m(F)$-module and then as a left R-module by extension of scalars. Observe that $M_m(F) \cong \mathrm{End}_F(F^m)$ and $M_{m,n}(F) \cong \mathrm{Hom}(F^n, F^m)$. Furthermore $F \cong \mathrm{End}({}_RI)$ and hence $S = \mathrm{End}_R I^n \cong M_n(F) \cong \mathrm{End}_F(F^n)$. As $I^n \subseteq \mathrm{Soc}({}_RR) \subseteq R$, every element $s \in S$ can be seen as homomorphism from a left ideal of R to R. Thus, as ${}_RR$ is injective, by Baer Criterion (Theorem 6.3), for every $s \in S$ there is $r \in R$ such that $xs = xr$ for every $x \in I^n$. We have $|Rx| = |I| = |F|^m$. On the other hand, identifying ${}_RI$ with the first column of $M_{m,n}(F)$ and taking x the matrix having 1 in the $(1,1)$ entry and zero in all the other entries. Then xS is the first row of $M_{m,n}(F)$ and it is contained in xR (after some identification of I^n inside R). Thus

$$\frac{|Rx|}{|xR|} \leq \frac{|F|^m}{|F|^n} < 1.$$

Therefore

$$|I|\,|\mathrm{r}(I)| = \frac{|Rx|}{|xR|}|R| < |R|,$$

as desired. □

12.3. Theorem [DLP04, Woo09] *The following conditions are equivalent for a finite ring R.*

1. *R is Frobenius.*
2. *The left and right annihilators of the standard bilinear map of R satisfies the following conditions:*
   (a) *For every positive integer n and every sumodule C of ${}_RR^n$ we have $\mathrm{l}(\mathrm{r}(C)) = C$ and $|C|\,|\mathrm{r}(C)| = |R|^n$.*
   (b) *For every positive integer n and every sumodule D of R_R^n we have $\mathrm{r}(\mathrm{l}(D)) = D$ and $|D|\,|\mathrm{l}(D)| = |R|^n$.*

   Moreover, in that case the MacWilliams identities hold: i.e.

$$W_{\mathrm{r}(C)}(X,Y) = \frac{1}{|C|}W_C(X + (|R|-1)Y, X - Y) \quad \textit{and} \quad W_{\mathrm{l}(D)}(X,Y) = \frac{1}{|R|}W_C(X + (|R|-1)Y, X - Y).$$

Proof. 1 implies 2. Suppose that R is Frobenius. Then there is $\chi \in R^*$ which generates ${}_RR^*$. By Lemma 9.1, χ also generates ${}_RR^*$ and χ does not contain any non-zero left or right ideal of R. By Theorem 11.1, statement 2 and the MacWilliams Identities hold.

2 implies 1. Suppose that R satisfies 2. In particular $\mathrm{l}(\mathrm{r}(I)) = I$ for every left ideal I of R and $\mathrm{r}(\mathrm{l}(I)) = I$ for every right ideal J of R. In other words R satisfies the double annihilator condition. Moreover, $|I|\,|\mathrm{r}(I)| = |R|$ for every left ideal I of R. Then R is Frobenius by Theorem 12.2. □

References

[AF92] F. W. Anderson and K. R. Fuller, *Rings and categories of modules*, second ed., Graduate Texts in Mathematics, vol. 13, Springer-Verlag, New York, 1992. MR 1245487 (94i:16001)

[DLP04] H. Q. Dinh and S. R. López-Permouth, *On the equivalence of codes over finite rings*, Appl. Algebra Engrg. Comm. Comput. **15** (2004), no. 1, 37–50. MR 2142429 (2006d:94097)

[GNW04] M. Greferath, A. Nechaev, and R. Wisbauer, *Finite quasi-Frobenius modules and linear codes*, J. Algebra Appl. **3** (2004), no. 3, 247–272. MR 2096449 (2005g:94099)

[Hon01] T. Honold, *Characterization of finite Frobenius rings*, Arch. Math. (Basel) **76** (2001), no. 6, 406–415. MR 1831096 (2002b:16033)

[Mac61] J. A. MacWilliams, *Error-correcting codes for multiple-level transmission*, Bell System Tech. J. **40** (1961), 281–308. MR 0141541 (25 #4945)

[Mac62] ———, *Combinatorial properties of finite abelian groups*, 1962, Thesis (Ph.D.)–Radcliffe College, Cambridge.

[Mac63] ———, *A theorem on the distribution of weights in a systematic code*, Bell System Tech. J. **42** (1963), 79–94. MR 0149978 (26 #7462)

[Pie82] R. S. Pierce, *Associative algebras*, Graduate Texts in Mathematics, vol. 88, Springer-Verlag, New York, 1982, Studies in the History of Modern Science, 9. MR 674652 (84c:16001)

[Woo09] J. A. Wood, *Foundations of linear codes defined over finite modules: the extension theorem and the MacWilliams identities*, Codes over rings, Ser. Coding Theory Cryptol., vol. 6, World Sci. Publ., Hackensack, NJ, 2009, pp. 124–190. MR 2850303 (2012h:94211)

Ángel del Río, Departamento de Matemáticas, Universidad de Murcia, 30100, Murcia, Spain
E-mail address: adelrio@um.es