LINEAR MATHEMATICS

Abstract. Exact sequences, products, coproducts, biproducts, matrices. Rings and modules.

1. Abelian groups and rings

1.1. **Abelian groups.** Generally, abelian groups A will now be written in additive notation $(A, +, 0)$, with unary negation as inversion and a zero element as identity. Powers are written as multiples. Recall that each subgroup C of an abelian group A is normal, so an abelian quotient group $A/C = \{a + C \mid a \in A\}$ is always well-defined, with addition $(a_1 + C) + (a_2 + C) = (a_1 + a_2) + C$, negation $-(a + C) = -a + C$, zero element $0 = C$, and (*natural*) *projection* $A \to A/C; a \mapsto a + C$. The trivial (abelian) group $\{0\}$ is often written simply as 0. For any abelian group A, there is a unique homomorphism $0 \to A$ and a unique homomorphism $A \to 0$.

1.1.1. *Exact sequences.*

Definition 1.1. Let $h\colon A \to B$ be a homomorphism of abelian groups.

(a) The *group kernel* of h is the subgroup

$$\operatorname{Ker} h = \{a \in A \mid ah = 0\}$$

of the domain A, together with the injection

$$\operatorname{Ker} h \to A\,. \tag{1.1}$$

(b) The *image* of h is the subgroup

$$\operatorname{Im} h = \{ah \in B \mid a \in A\}$$

of the codomain B.

(c) The *cokernel* of h is the quotient group

$$\operatorname{Coker} h = B/\operatorname{Im} h$$

of the codomain B, together with the projection

$$B \to \operatorname{Coker} h\,. \tag{1.2}$$

In Definition 1.1, note the duality between the injection $\operatorname{Ker} h \to A$ and the projection $B \to \operatorname{Coker} h$.

Definition 1.2. Consider a sequence

$$A_0 \longrightarrow \ldots \xrightarrow{f_{n-2}} A_{n-1} \xrightarrow{f_{n-1}} A_n \xrightarrow{f_n} A_{n+1} \xrightarrow{f_{n+1}} \ldots \longrightarrow A_N$$

of abelian group homomorphisms.

(a) The sequence is said to be *exact at* A_n if $\operatorname{Im} f_{n-1} = \operatorname{Ker} f_n$.
(b) The sequence is said to be *exact* whenever it is exact at each intermediate group $A_1, \ldots, A_{N-1}$.

Proposition 1.3 (Extended First Isomorphism Theorem)**.** *Suppose that $h\colon A \to B$ is a homomorphism of abelian groups. Then there is an exact sequence*

$$0 \longrightarrow \operatorname{Ker} h \longrightarrow A \xrightarrow{h} B \longrightarrow \operatorname{Coker} h \longrightarrow 0$$

with the injection (1.1) *and projection* (1.2)*.*

1.1.2. *Groups of homomorphisms.* For sets X and Y, the morphism class $\mathbf{Set}(X, Y)$ of functions from X to Y is a set. Let $\underline{\underline{\mathbb{Z}}}$ denote the category of abelian groups and homomorphisms. For abelian groups A and B, the set $\underline{\underline{\mathbb{Z}}}(A, B)$ is an abelian group, a subgroup of the power group B^A with componentwise operations. The zero 0 of $\underline{\underline{\mathbb{Z}}}(A, B)$ is the composite $A \to 0 \to B$. The identity function on the abelian group A is written as 1 in $\underline{\underline{\mathbb{Z}}}(A, A)$.

Proposition 1.4. *Suppose that A, B, C, A_i are abelian groups (for i in an index set I).*

(a) *There is an abelian group isomorphism $\underline{\underline{\mathbb{Z}}}(\mathbb{Z}, A) \cong A$.*
(b) *There is an abelian group isomorphism*

$$\underline{\underline{\mathbb{Z}}}(C, A \times B) \cong \underline{\underline{\mathbb{Z}}}(C, A) \times \underline{\underline{\mathbb{Z}}}(C, B)\,.$$

(c) *There is an abelian group isomorphism*

$$\underline{\underline{\mathbb{Z}}}\Big(C, \prod_{i \in I} A_i\Big) \cong \prod_{i \in I} \underline{\underline{\mathbb{Z}}}(C, A_i)\,.$$

1.1.3. *Biproducts.* Suppose that $A_1, \ldots, A_m, C$ are abelian groups, with homomorphisms $f_i\colon A_i \to C$ for $1 \le i \le m$. Consider the *insertions*

$$\iota_j\colon A_j \to \prod_{i=1}^{m} A_i; a_j \mapsto (0, \ldots, 0, \overbrace{a_j}^{\text{Slot}\,j}, 0, \ldots, 0) \tag{1.3}$$

for $1 \le j \le m$. Then

$$\sum_{i=1}^{m} f_i\colon \prod_{i=1}^{m} A_i \to C; (a_1, \ldots, a_m) \mapsto \sum_{i=1}^{m} a_i f_i$$

is the unique homomorphism $f\colon \prod_{i=1}^m A_i \to C$ such that $\iota_j f = f_j$ for each $1 \leq j \leq m$. In other words, the product $\prod_{i=1}^m A_i$, with the insertions ι_i, is the *coproduct* of the groups A_i, $1 \leq i \leq m$. For this reason, the product $\prod_{i=1}^m A_i$ is described as the *biproduct* or *external direct sum* $\bigoplus_{i=1}^m A_i$ of the groups A_i (and occasionally as the *internal direct sum* of its embedded subgroups $A_i\iota_i$).

1.1.4. *Matrices.* Let $A_1, \ldots, A_m$ and $B_1, \ldots, B_n$ be abelian groups. Each element f of $\underline{\underline{\mathbb{Z}}}\left(\bigoplus_{i=1}^m A_i, \bigoplus_{j=1}^n B_j\right)$ determines an $m \times n$-*matrix*

$$[f] = \begin{bmatrix} \iota_1 f \pi_1 & \ldots & \iota_1 f \pi_n \\ & \ldots \quad \iota_i f \pi_j \quad \ldots & \\ \iota_m f \pi_1 & \ldots & \iota_m f \pi_n \end{bmatrix} \tag{1.4}$$

with (i,j)-*entries* $\iota_i f \pi_j\colon A_i \to B_j$. Conversely, each $m \times n$-matrix

$$F = \begin{bmatrix} f_{11} & \ldots & f_{1n} \\ & \ldots \quad f_{ij} \quad \ldots & \\ f_{m1} & \ldots & f_{mn} \end{bmatrix}$$

with entries $f_{ij} \in \underline{\underline{\mathbb{Z}}}(A_i, B_j)$ determines a unique homomorphism

$$f\colon \bigoplus_{i=1}^m A_i \to \bigoplus_{j=1}^n B_j$$

whose matrix (1.4) is F (Exercise 8).

1.1.5. *Coproducts.* Let I be an arbitrary index set. Consider abelian groups A_i for $i \in I$. A coproduct of the groups A_i is constructed within the product $\prod_{j\in I} A_j$. Given i in I, an insertion $\iota_i\colon A_i \to \prod_{j\in I} A_j$ is defined as the product $\prod_{j\in I} \delta_{ij}\colon A_i \to \prod_{j\in I} A_j$ of the homomorphisms $\delta_{ij} \in \underline{\underline{\mathbb{Z}}}(A_i, A_j)$ with $\delta_{ii} = 1$ and $\delta_{ij} = 0$ for $i \neq j$ — compare (1.3). Then the *coproduct* $\coprod_{j\in I} A_j$ is defined as the subgroup of $\prod_{j\in I} A_j$ generated be the subset $\bigcup\{A_i\iota_i \mid i \in I\}$. Given homomorphisms $f_i\colon A_i \to C$ for $i \in I$, with common codomain C, a unique homomorphism $\sum_{i\in I} f_i$ or $f\colon \coprod_{j\in I} A_j \to C$, with $\iota_i f = f_i$ for $i \in I$, is defined by

$$f\colon \sum_{j=1}^n a_{i_j} \mapsto \sum_{j=1}^n a_{i_j} f_{i_j}$$

for $a_{i_j} \in A_{i_j}$, $1 \leq j \leq n$. Note that $\coprod_{j\in I} A_j$ is a proper subgroup of $\prod_{j\in I} A_j$ if infinitely many of the groups A_i are non-trivial (compare Exercise 13).

1.2. **Rings.** Let A be an abelian group. The linear analogue of the set X^X of all functions on a set X is the set $\underline{\underline{\mathbb{Z}}}(A, A)$ of homomorphisms from A to A. Such homomorphisms are known as *endomorphisms*, and $\underline{\underline{\mathbb{Z}}}(A, A)$ is written as $\operatorname{End} A$. As noted in §1.1.2, there is a componentwise abelian group structure $(\operatorname{End} A, +, 0)$. On the other hand, $\operatorname{End} A$ is a submonoid of $(A^A, \cdot, 1)$.

Definition 1.5. Let $(S, +, 0)$ be an abelian group.

(a) If there is a semigroup structure $(S, \cdot)$ such that all the right multiplications

$$R(s)\colon S \to S; x \mapsto xs \tag{1.5}$$

and left multiplications

$$L(s)\colon S \to S; x \mapsto sx \tag{1.6}$$

by elements s of S are endomorphisms of $(S, +, 0)$, then S is said to be a (*non-unital*) *ring* $(S, +, \cdot)$.

(b) If there is a monoid structure $(S, \cdot, 1)$ such that $(S, +, \cdot)$ is a non-unital ring, then S is said to be a (*unital*) *ring* $(S, +, \cdot, 1)$.

(c) A ring $(S, +, \cdot)$ is *commutative* whenever the semigroup $(S, \cdot)$ is commutative.

In Definition 1.5(a), the endomorphism conditions on the right and left multiplications are described as *right* and *left distributivity*.

Example 1.6. For an abelian group A, the set $\operatorname{End} A$ forms a unital ring $(\operatorname{End} A, +, \cdot, 1)$. Indeed, for elements $a \in A$ and $r, s, t \in \operatorname{End} A$, one has

$$a(r + s)t = (ar + as)t = art + ast = a(rt + st)$$

and

$$at(r + s) = atr + ats = a(tr + ts)\,,$$

so $(r + s)t = rt + rt$ and $t(r + s) = tr + ts$ as required.

Example 1.7. Let A be an abelian group. Define $a \cdot b = 0$ for all $a, b \in A$. Then $(A, +, \cdot)$ is a non-unital ring, known as a *zero ring*.

Definition 1.8. Let S be a unital ring.

(a) S is a(n *integral*) *domain* if $(S \smallsetminus \{0\}, \cdot, 1)$ is a commutative monoid.

(b) S is a *skewfield* if $(S \smallsetminus \{0\}, \cdot, 1)$ is a group.

(c) S is a *field* if $(S \smallsetminus \{0\}, \cdot, 1)$ is a commutative group.

Example 1.9. (a) $\mathbb{Z}$ forms an integral domain.

(b) $\mathbb{R}$ and $\mathbb{C}$ form fields.

(c) $\mathbb{Z}/_n$ forms a field iff n is prime.

Definition 1.10. Let S or $(S, +, \cdot)$ be a ring. Then the *opposite ring* S^{op} is the ring $(S, +, \circ)$ with $x \circ y = y \cdot x$ for $x, y \in S$.

1.2.1. *Matrix rings.* Let S be a ring. For positive integers m and n, the set of all $m \times n$-matrices with entries in S is written as S^n_m. As an implementation of the power S^{mn}, the set S^n_m has componentwise ring structure. The componentwise product is called the *Hadamard product*. On the other hand, the usual matrix multiplication (compare Exercise 9) gives a product $S^n_m \times S^p_n \to S^p_m$ for positive integers m, n, p. Equipped with this product and componentwise addition, the set S^n_n of all $n \times n$-matrices over S forms a ring $(S^n_n, +, \cdot)$, known as the $n \times n$ *matrix ring* over S. If S is unital, then $(S^n_n, +, \cdot, I_n)$ is unital with the $n \times n$ *identity matrix* having 1 in each diagonal entry and 0 in each off-diagonal position.

1.2.2. *The algebra of rings.* Since rings are algebras, the usual algebraic notions apply. It is sometimes necessary to distinguish carefully between the unital and non-unital cases when discussing subrings and ring homomorphisms, although the distinction is often left implicit.

Definition 1.11. Let S be a ring.

(a) A subgroup J of $(S, +, 0)$ is said to be an *ideal*, written $J \lhd S$, if the *absorption properties*

$$\forall\ j \in J\,,\ \forall\ s \in S\,,\ js \in J \text{ and } sj \in J$$

are satisfied.

(b) The *ring kernel* of a ring homomorphism $f\colon S \to T$ is the group kernel $\operatorname{Ker} f = \{s \in S \mid sf = 0\}$.

Proposition 1.12. *Let S be a ring.*

(a) *Each ring kernel in S is an ideal of S.*

(b) *For $J \lhd S$, the quotient group S/J has a well-defined multiplication making the group projection*

$$S \to S/J; s \mapsto s + J$$

a ring homomorphism.

Definition 1.13. Let S be a ring.

(a) The *trivial* ideal is $\{0\}$ and the *improper* ideal is S.

(b) The ring S is *simple* if its only ideals are trivial or improper.

Proposition 1.14. *Let S be a commutative, unital ring. Then S is a field if and only if it is simple and non-trivial.*

2. Modules

Modules over a ring are the linear analogues of sets with a semigroup or monoid action. In particular, abelian groups are modules over $\mathbb{Z}$, while real vector spaces are modules over $\mathbb{R}$.

2.1. **Unital modules.**

Definition 2.1. Let S be a ring.

(a) If A is an abelian group with a non-unital ring homomorphism

$$r\colon S \to \operatorname{End} A; s \mapsto (A \to A; a \mapsto as)\,, \tag{2.1}$$

then A is said to be a (*non-unital*) (*right*) *S-module*.

(b) If A is an abelian group with a non-unital ring homomorphism

$$l\colon S^{\mathsf{op}} \to \operatorname{End} A; s \mapsto (A \to A; a \mapsto sa)\,, \tag{2.2}$$

then A is said to be a (*non-unital*) *left S-module*.

(c) If (2.1) is a unital ring homomorphism, then A is said to be a (*unital*) (*right*) *S-module*.

(d) If (2.2) is a unital ring homomorphism, then A is said to be a (*unital*) (*left*) *S-module*.

(e) An abelian group homomorphism $f\colon (A,+,0) \to (B,+,0)$ is a (*right* or *left*) *S-module homomorphism* $f\colon (A,+,S) \to (B,+,S)$ if it is a (right or left) S-set homomorphism.

(f) If K is a field, then a K-module is called a *vector space* over K, and K-module homomorphisms are often described as *linear transformations*.

Example 2.2. Let S be a ring. Consider the matrix notation of §1.2.1. Then for positive integers m and n, the abelian group S_m^n becomes a left S_m^m-module and a right S_n^n-module under the usual matrix multiplication.

For a (unital) ring S, the category of (unital) right S-modules and homomorphisms is written as $\mathbf{Mod}_S$ or $\underline{\underline{S}}$. [This is the reason for the notation introduced in §1.1.2 for the category of abelian groups.] The category of (unital) left S-modules and homomorphisms is written as ${}_S\mathbf{Mod}$. For a commutative ring S, there is no essential distinction between left and right S-modules.

In many aspects of linear algebra over the field $\mathbb{R}$ of real numbers, the only relevant property of $\mathbb{R}$ is the field property. Thus the results and concepts of elementary linear algebra (bases, linear independence, dimension, etc.) apply equally to vector spaces over a general field K.

2.1.1. *The algebra of modules.* For a ring S, a set A that is both an abelian group and a right S-set is a right S-module if and only if $(a+b)s = as + bs$ for elements a, b in A and "scalars" $s \in S$. Since S-modules are algebras, the usual algebraic notions apply. If H is a submodule of a module A, then the group quotient A/H carries a well-defined S-module structure — with $(a+H)s = as + H$ for $a \in A$, $s \in S$ — such that the projection $A \to A/H; a \mapsto a + H$ becomes an S-module homomorphism. All the definitions of §1.1.1 (cokernels, exact sequences, ...) carry over, so the Extended First Isomorphism Theorem (Proposition 1.3) holds for S-modules (Exercise 20).

Given S-modules A_i (for i in an index set I), the product $\prod_{i\in I} A_i$ is the product both of the abelian groups A_i and the S-sets A_i. In other words, given S-homomorphisms $f_i\colon C \to A_i$ with common domain C, there is a unique S-homomorphism $f\colon C \to \prod_{i\in I} A_i$ such that $f\pi_i = f_i$ for each $i \in I$. Now the abelian group coproduct $\coprod_{i\in I} A_i$ is an S-subset of the S-set $\prod_{i\in I} A_i$, and thus an S-module. It is the *coproduct* of the S-modules A_i: Given S-homomorphisms $f_i\colon A_i \to C$ with common codomain C, there is a unique S-homomorphism $f\colon \coprod_{i\in I} A_i \to C$ such that $\iota_i f = f_i$ for each $i \in I$. If there are only finitely many non-trivial modules A_i, then the product and coproduct coincide to give the *biproduct* $\bigoplus_{i\in I} A_i$. In particular, the matrix notation of §1.1.4 applies to elements of $\underline{\underline{\mathbb{S}}}\left(\bigoplus_{i=1}^m A_i, \bigoplus_{j=1}^n B_j\right)$.

2.1.2. *Schur's Lemma.* Let S be a unital ring. For S-homomorphisms $f\colon A \to B$ and $g\colon A \to B$, the sum $f+g$ is an S-homomorphism. Thus $\underline{\underline{S}}(A, A)$ is an abelian subgroup of $\underline{\underline{Z}}(A, A)$.

Definition 2.3. A unital right S-module A is *simple* if it has no proper, non-trivial submodules.

Proposition 2.4 (Schur's Lemma)**.** *Let A be a simple S-module. Then $\underline{\underline{S}}(A, A)$ is a skewfield.*

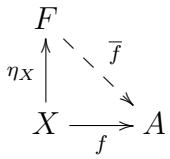
Proof. Consider an S-homomorphism $f\colon A \to A$. If the submodule $\operatorname{Ker} f$ is non-trivial, one has $\operatorname{Ker} f = A$ and $f = 0$. Otherwise, $\operatorname{Ker} f = \{0\}$ and f is injective. Since $f \neq 0$, the submodule $\operatorname{Im} f$ of A is non-trivial. Thus $\operatorname{Im} f = A$ and f is surjective. Thus f is invertible, and $f^{-1} \in \underline{\underline{S}}(A, A)$. □

2.2. **Free and projective modules.**

2.2.1. *Free modules.* Let S be a ring. An S-module F is said to be a *free module* over a set X if there is a function $\eta_X\colon X \to F$ such that

each function $f\colon X \to A$ to an S-module A extends uniquely to an S-homomorphism $\overline{F}\colon F \to A$ such that $\eta_X f = \overline{f}$.

(2.3)



Specifically, one speaks of free right and left S-modules in the respective contexts of right and left S-modules.

Proposition 2.5. *Let S be a unital ring.*

(a) *With scalar multiplications* (1.5) *for $s \in S$, the ring S becomes a unital right S-module, written as S or S_S.*
(b) *With $\eta_{\{x\}}\colon \{x\} \to S_S; x \mapsto 1$, the module S_S becomes a free unital right S-module over a singleton $\{x\}$.*
(c) *With scalar multiplications* (1.6) *for $s \in S$, the ring S becomes a unital left S-module, written as S or ${}_SS$.*
(d) *With $\eta_{\{x\}}\colon \{x\} \to_S S; x \mapsto 1$, the module ${}_SS$ becomes a free unital left S-module over $\{x\}$.*

Definition 2.6. Let S be a unital ring.

(a) A submodule of S_S is called a *right ideal* of S.
(b) A submodule of ${}_SS$ is called a *left ideal* of S.

If S_S is playing the role of the free right S-module over $\{x\}$, as in Proposition 2.5(b), it is convenient to write it as $xS = \{xs \mid s \in S\}$ with $x1 = x$ and an S-module isomorphism $S \to xS; s \mapsto xs$, taking $\eta_{\{x\}}\colon \{x\} \to xS; x \mapsto x$.

Corollary 2.7. *Let X be a set. Then the coproduct $\sum_{x\in X} xS$ is the free right S-module over X, with $\eta_X\colon X \to \sum_{x\in X} xS; x \mapsto x\eta_{\{x\}}\iota_x$. Given a function $f\colon X \to A$ from X to an S-module A, the map*

$$\overline{f}\colon \sum_{x\in X} xS \to A; \sum_{j=1}^{n} x_j s_j \mapsto \sum_{j=1}^{n} x_j f s_j$$

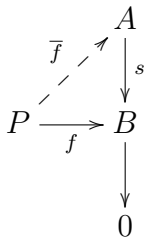
is the unique S-homomorphic extension of $f\colon X \to A$.

2.2.2. *Projective modules.*

Definition 2.8. Let S be a unital ring. A S-module P is said to be *projective* if for each S-homomorphism $f\colon P \to B$ and surjective S-homomorphism $s\colon A \to B$, there is an S-homomorphism $\overline{f}\colon P \to A$ such that $\overline{f}s = f$. Each such homomorphism $\overline{f}$ is called a *lifting* of f from B to A.

Definition 2.8 may be illustrated as follows:

(2.4)



The right hand side of the picture is understood as an exact sequence, expressing the surjectivity of s — compare Definition 1.2(a). Note that the lifting $\overline{f}$ of f is not required to be unique.

Proposition 2.9. *Let S be a unital ring.*

(a) *A free S-module is projective.*
(b) *An S-module P is projective if and only if there is a free S-module F with an isomorphism $F \cong P \oplus Q$.*

Proof. For (a), suppose that P is free over X. Consider the situation of (2.4). Let $r\colon B \to A$ be a retract for $s\colon A \to B$. Then $\overline{f}\colon P \to A$ is the unique homomorphic extension of the restriction of fr to $X\eta_X$. The proof of (b) is left as Exercise 22. □

Example 2.10. By Proposition 2.9(b), the $(\mathbb{Z}\times\mathbb{Z})$-module $\mathbb{Z}\times\{0\}$ is projective (but not free).

2.3. **Duality.**

Proposition 2.11. *Consider a unital ring S and an abelian group G.*

(a) *Let A be a right S-module. Then the abelian group $\underline{\underline{\mathbb{Z}}}(A,G)$, with scalar multiplications defined by the mixed associative law*

$$a(s\alpha) = (as)\alpha$$

for $a \in A$, $s \in S$, $\alpha \in \underline{\underline{\mathbb{Z}}}(A,G)$, is a left S-module.

(a) *Let B be a left S-module. Then the abelian group $\underline{\underline{\mathbb{Z}}}(B,G)$, with scalar multiplications defined by the mixed associative law*

$$(\beta s)(b) = \beta(sb)$$

for $b \in A$, $s \in S$, $\beta \in \underline{\underline{\mathbb{Z}}}(B,G)$, is a right S-module.

Definition 2.12. The modules $A^T = \underline{\underline{\mathbb{Z}}}(A,G)$ and $B^T = \underline{\underline{\mathbb{Z}}}(B,G)$ of Proposition 2.11 are known as the modules *dual* to the respective modules A and B.

Example 2.13. Given S-modules A_i (for i in an index set I), there is an abelian group isomorphism

$$\theta\colon \underline{\underline{\mathbb{Z}}}\Big(\coprod_{i\in I} A_i, G\Big) \to \prod_{i\in I} \underline{\underline{\mathbb{Z}}}(A_i, G)\,,$$

where $\big(\sum_{i\in I} f_i\big)\theta$ is determined by its projections $\big(\sum_{i\in I} f_i\big)\theta\pi_j = f_j$ for $j \in I$. Now for $s \in S$, one has

$$\big(s\sum_{i\in I} f_i\big)\theta\pi_j = \big(\sum_{i\in I} sf_i\big)\theta\pi_j = sf_j\,,$$

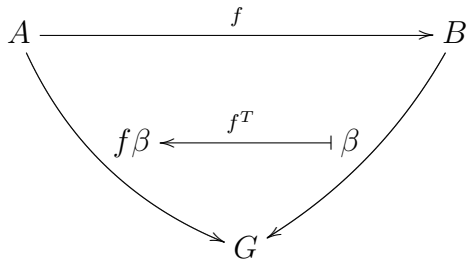
whence $\big(s\sum_{i\in I} f_i\big)\theta = s\big((\sum_{i\in I} f_i)\theta\big)$, and θ becomes a left S-module homomorphism. In other words, the dual $\big(\coprod_{i\in I} A_i\big)^T$ of the coproduct is (isomorphic to) the product $\prod_{i\in I} A_i^T$ of the duals.

Example 2.14. Let S be a unital ring, and let G be the abelian group $(S, +, 0)$. Consider the free right S-module S_S of Proposition 2.5(a). Define

$$R\colon S \to S_S^T; t \mapsto \big(R(t)\colon S \to S; s \mapsto st\big)\,.$$

For $x, s, t \in S$, one has $x\big(sR(t)\big) = (xs)R(t) = (xs)t = x(st) = xR(st)$ and $t = 1R(t)$. Thus R is a left S-module homomorphism embedding the free left S-module ${}_SS$ of Proposition 2.5(c) as a submodule of the dual S_S^T.

2.3.1. *Dual homomorphisms.* Fix a unital ring S and an abelian group G. Let $f\colon A \to B$ be a homomorphism of right S-modules. Then, as illustrated below,



a map $\underline{\underline{Z}}(f, G)$ or f^T is defined as $f^T\colon B^T \to A^T; \beta \mapsto f\beta$. This map, which is a left S-module homomorphism (Exercise 26), is defined as the *dual* of the S-homomorphism f. Given a further S-homomorphism $g\colon B \to C$, one has $(fg)^T = g^T f^T$. Dual homomorphisms are often written with Eulerian notation, so that this relationship takes the form $(fg)^T = f^T \circ g^T$. In general, duality in linear mathematics means applying the construction $\underline{\underline{Z}}(\_, G)$.

2.3.2. *Transposes of matrices.* Fix a unital ring S and an abelian group G. For given right S-modules $A_1, \dots, A_m$ and $B_1, \dots, B_n$, consider an element f of $\underline{\underline{S}}\left(\bigoplus_{i=1}^m A_i, \bigoplus_{j=1}^n B_j\right)$. Recall that f has a matrix $[f]$ as in §1.1.4, with (i,j)-entries f_{ij} or $\iota_i f \pi_j \colon A_i \to B_j$. By Example 2.13, one obtains

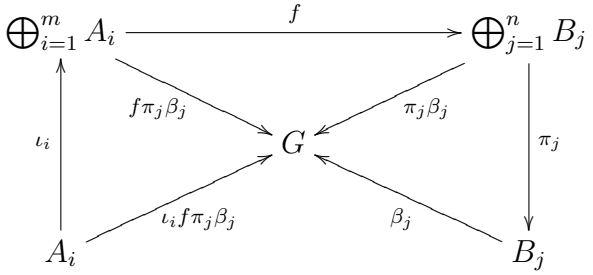
$$\left(\bigoplus_{i=1}^m A_i\right)^T = \underline{\underline{S}}\left(\bigoplus_{i=1}^m A_i, G\right) = \underline{\underline{S}}\left(\coprod_{i=1}^m A_i, G\right)$$
$$\cong \prod_{i=1}^m \underline{\underline{S}}\,(A_i, G) = \bigoplus_{i=1}^m \underline{\underline{S}}\,(A_i, G) = \bigoplus_{i=1}^m A_i^T$$

and $\left(\bigoplus_{j=1}^n B_j\right)^T \cong \bigoplus_{j=1}^n B_j^T$, the isomorphisms being homomorphisms of left S-modules. Thus f^T, which *a priori* is an element of the group

$$\underline{\underline{\mathbb{Z}}}\left(\left(\bigoplus_{j=1}^n B_j\right)^T, \left(\bigoplus_{i=1}^m A_i\right)^T\right),$$

becomes an element of $\underline{\underline{\mathbb{Z}}}\left(\bigoplus_{j=1}^n B_j^T, \bigoplus_{i=1}^m A_i^T\right)$. Two questions then arise: What is the $n \times m$-matrix $[f^T]$ of f^T, and what relationship does that matrix $[f^T]$ bear to the $m \times n$-matrix $[f]$ of f?

To answer these questions, consider $\beta_j \in B_j^T$ for $1 \le j \le n$ and $1 \le i \le m$ in the following commutative diagram:



Then under the composite $B_j^T \xrightarrow{\iota_j} \bigoplus_{k=1}^n B_k \xrightarrow{f^T} \bigoplus_{h=1}^m A_h \xrightarrow{\pi_i} A_i^T$, the element β_j maps to $\iota_i f \pi_j \beta_j = f_{ij}\beta_j = f_{ij}^T(\beta_j)$. Thus:

Theorem 2.15. *If $f \in \underline{\underline{S}}\left(\bigoplus_{i=1}^m A_i, \bigoplus_{j=1}^n B_j\right)$ has $m \times n$-matrix $[f_{ij}]$, the dual homomorphism $f^T \in \underline{\underline{\mathbb{Z}}}\left(\bigoplus_{j=1}^n B_j^T, \bigoplus_{i=1}^m A_i^T\right)$ has an $n \times m$-matrix whose (j,i)-entry is the dual f_{ij}^T of the (i,j)-entry f_{ij} of $[f]$.*

In Theorem 2.15, the $n \times n$-matrix $[f^T]$ is called the *transpose* of the $m \times n$-matrix $[f]$.

3. Exercises

(1) Let $h\colon A \to B$ be a homomorphism of abelian groups.
   (a) Prove that h is injective if and only if $\operatorname{Ker} h = 0$.
   (b) Prove that h is surjective if and only if $\operatorname{Coker} h = 0$.
   (b) Prove that h is an isomorphism if and only if the sequence $0 \to A \xrightarrow{h} B \to 0$ is exact.

(2) Let $0 \to A \to B \to C \to 0$ be an exact sequence of finite abelian groups. Prove that $\log|A| - \log|B| + \log|C| = 0$.

(3) Let $0 \to A_0 \to A_1 \to \cdots \to A_n \to 0$ an exact sequence of finite abelian groups. Prove that $\sum_{i=0}^{n}(-1)^i \log|A_i| = 0$.

(4) Prove the Extended First Isomorphism Theorem (Proposition 1.3).

(5) Give an example of groups G and H such that the set of group homomorphisms from G to H is not a subgroup of the power H^G (with componentwise operations).

(6) Prove Proposition 1.4.

(7) Let $A_1, \ldots, A_m, C$ be abelian groups. Show that

$$\underline{\underline{\mathbb{Z}}}\left(C, \bigoplus_{i=1}^{m} A_i\right) \cong \prod_{i=1}^{m} \underline{\underline{\mathbb{Z}}}(C, A_i)$$

and

$$\underline{\underline{\mathbb{Z}}}\left(\bigoplus_{i=1}^{m} A_i, C\right) \cong \prod_{i=1}^{m} \underline{\underline{\mathbb{Z}}}(A_i, C)\,.$$

(8) Prove the claim of §1.1.4.

(9) Let $A_1, \ldots, A_m$, $B_1, \ldots, B_n$, and $C_1, \ldots, C_p$ be abelian groups. Consider homomorphisms

$$f\colon \bigoplus_{i=1}^{m} A_i \to \bigoplus_{j=1}^{n} B_j \quad \text{and} \quad g\colon \bigoplus_{j=1}^{n} B_j \to \bigoplus_{k=1}^{p} C_k$$

with matrices $[f]$ and $[g]$. Determine the matrix $[fg]$ of

$$fg\colon \bigoplus_{i=1}^{m} A_i \to \bigoplus_{k=1}^{p} C_k$$

in terms of the entries f_{ij} and g_{jk}.

(10) Let $A, A_1, \ldots, A_m$ be abelian groups. Show that the group A is the biproduct of $A_1, \ldots, A_m$ if and only if there are homomorphisms $p_i\colon A \to A_i$ and $j_i\colon A_i \to A$ for $1 \le i \le m$ such that:
   (a) $\forall\ 1 \le h, i \le m\,,\ j_h p_i = \delta_{hi} 1_{A_i}$;
   (b) $1_A = \sum_{i=1}^{m} p_i j_i$ in $\underline{\underline{\mathbb{Z}}}(A, A)$.

(11) An exact sequence, with three groups sandwiched between zero groups, is called a *short exact sequence*. Let

$$0 \to A \xrightarrow{j} E \xrightarrow{p} Q \to 0$$

be a short exact sequence of abelian groups. In this context, E is called an *extension* of A by Q. Show that the following three conditions are equivalent:
   (a) The surjection $p\colon E \to Q$ has a section $s\colon Q \to E$ that is a homomorphism;
   (b) The injection $j\colon A \to E$ has a retract $r\colon E \to A$ that is a homomorphism;
   (c) The extension E is the internal direct sum of $\operatorname{Im} j$ and $\operatorname{Coker} j$.

   (If these conditions hold, the extension and the exact sequence are said to *split*).

(12) Let B be an abelian group. Consider subgroups B_i of B, with i in an index set I. Show that the subgroup of B generated by $\bigcup\{B_i \mid i \in I\}$ is

$$\left\{ \sum_{j=1}^{n} b_{i_j} \;\middle|\; n \in \mathbb{N}\,,\ 1 \le j \le n\,,\ i_j \in I\,,\ b_{i_j} \in B_{i_j} \right\}.$$

(13) For each natural number n, let A_n be a copy of the abelian group $\mathbb{Z}/_2$ of bits or integers modulo 2 under addition. Show that the set $\coprod_{n\in\mathbb{N}} A_n$ is countable, while the set $\prod_{n\in\mathbb{N}} A_n$ is uncountable.

(14) If a positive integer n is composite, show that $\mathbb{Z}/_n$ is not an integral domain.

(15) Complete the verification of the claims of §1.1.5.

(16) Let A be a zero ring. Show that the 2×2 matrix ring A_2^2 is commutative.

(17) Prove Proposition 1.12, and formulate the First Isomorphism Theorem for Rings.

(18) (a) Prove Proposition 1.14.
   (b) Give an example of a simple, non-trivial commutative ring which is not a field.

(19) Let S be a field. For $1 < n \in \mathbb{Z}$, show that S_n^n is a simple, non-trivial unital ring which is not a skewfield. [Hint: For $1 \le k, l \le n$, consider the *elementary matrices* E^{kl} with i,j-entry $[E^{kl}]_{ij} = \delta_{ik}\delta_{jl}$.]

(20) Let S be a unital ring. Formulate and prove the Extended First Isomorphism Theorem for right S-modules.

(21) (a) Prove Proposition 2.5 and Corollary 2.7.
(b) Formulate and prove the analogue of Corollary 2.7 for left S-modules.
(22) Complete the proof of Proposition 2.9.
(23) An element e of a ring S is said to be *idempotent* if $ee = e$. Suppose that e is an idempotent element of a unital ring S.
(a) Show that $eS = \{es \mid s \in S\}$ is a right ideal of S.
(b) Show that eS is a projective right S-module.
(24) Let A be a finitely generated abelian group. Use the structure theory for such groups to show that if A is projective, then it is free.
(25) Prove Proposition 2.11.
(26) Suppose that $f\colon A \to B$ is a right S-homomorphism. Show that $f^T\colon B^T \to A^T$ is a left S-homomorphism.
(27) For $1 < n \in \mathbb{Z}$, consider the abelian group $\mathbb{Z}/_n$ as a $\mathbb{Z}$-module. Let G be the *circle group*, the group $\{z \in \mathbb{C} \mid z\overline{z} = 1\}$ of complex numbers of unit modulus. Show that $\mathbb{Z}/_n$ is isomorphic with its dual $\mathbb{Z}/_n^T$.