Part IV

Algebra: PID's, UFD's, Noetherian Rings, Tensors, Modules over a PID, Normal Forms

Chapter 30

Polynomials, Ideals and PID's

30.1 Multisets

This chapter contains a review of polynomials and their basic properties. First, multisets are defined. Polynomials in one variable are defined next. The notion of a polynomial function in one argument is defined. Polynomials in several variable are defined, and so is the notion of a polynomial function in several arguments. The Euclidean division algorithm is presented, and the main consequences of its existence are derived. Ideals are defined, and the characterization of greatest common divisors of polynomials in one variables (gcd's) in terms of ideals is shown. We also prove the Bezout identity. Next, we consider the factorization of polynomials in one variables into irreducible factors. The unique factorization of polynomials in one variable into irreducible factors is shown. Roots of polynomials and their multiplicity are defined. It is shown that a nonnull polynomial in one variable and of degree m over an integral domain has at most m roots. The chapter ends with a brief treatment of polynomial interpolation: Lagrange, Newton, and Hermite interpolants are introduced.

In this chapter, it is assumed that all rings considered are commutative. Recall that a (commutative) ring A is an *integral domain* (or an *entire ring*) if $1 \neq 0$, and if $ab = 0$, then either $a = 0$ or $b = 0$, for all $a, b \in A$. This second condition is equivalent to saying that if $a \neq 0$ and $b \neq 0$, then $ab \neq 0$. Also, recall that $a \neq 0$ is *not* a zero divisor if $ab \neq 0$ whenever $b \neq 0$. Observe that a field is an integral domain.

Our goal is to define polynomials in one or more indeterminates (or variables) $X_1, \ldots, X_n$, with coefficients in a ring A. This can be done in several ways, and we choose a definition that has the advantage of extending immediately from one to several variables. First, we need to review the notion of a (finite) multiset.

Definition 30.1. Given a set I, a *(finite) multiset over I* is any function $M \colon I \to \mathbb{N}$ such that $M(i) \neq 0$ for finitely many $i \in I$. The multiset M such that $M(i) = 0$ for all $i \in I$ is the *empty multiset*, and it is denoted by 0. If $M(i) = k \neq 0$, we say that *i is a member of M of multiplicity k.* The *union* $M_1 + M_2$ of two multisets M_1 and M_2 is defined such that $(M_1 + M_2)(i) = M_1(i) + M_2(i)$, for every $i \in I$. If I is finite, say $I = \{1, \ldots, n\}$, the multiset

M such that $M(i) = k_i$ for every i, $1 \leq i \leq n$, is denoted by $k_1 \cdot 1 + \cdots + k_n \cdot n$, or more simply, by $(k_1, \ldots, k_n)$, and $\deg(k_1 \cdot 1 + \cdots + k_n \cdot n) = k_1 + \cdots + k_n$ is the *size* or *degree* of M. The set of all multisets over I is denoted by $\mathbb{N}^{(I)}$, and when $I = \{1, \ldots, n\}$, by $\mathbb{N}^{(n)}$.

Intuitively, the order of the elements of a multiset is irrelevant, but the multiplicity of each element is relevant, contrary to sets. Every $i \in I$ is identified with the multiset M_i such that $M_i(i) = 1$ and $M_i(j) = 0$ for $j \neq i$. When $I = \{1\}$, the set $\mathbb{N}^{(1)}$ of multisets $k \cdot 1$ can be identified with $\mathbb{N}$ and $\{1\}^*$. We will denote $k \cdot 1$ simply by k.

However, beware that when $n \geq 2$, the set $\mathbb{N}^{(n)}$ of multisets cannot be identified with the set of strings in $\{1, \ldots, n\}^*$, because multiset union is commutative, but concatenation of strings in $\{1, \ldots, n\}^*$ is not commutative when $n \geq 2$. This is because in a multiset $k_1 \cdot 1 + \cdots + k_n \cdot n$, the order is irrelevant, whereas in a string, the order is relevant. For example, $2 \cdot 1 + 3 \cdot 2 = 3 \cdot 2 + 2 \cdot 1$, but $11222 \neq 22211$, as strings over $\{1, 2\}$.

Nevertheless, $\mathbb{N}^{(n)}$ and the set $\mathbb{N}^n$ of ordered n-tuples under component-wise addition are isomorphic under the map

$$k_1 \cdot 1 + \cdots + k_n \cdot n \mapsto (k_1, \ldots, k_n).$$

Thus, since the notation $(k_1, \ldots, k_n)$ is less cumbersome that $k_1 \cdot 1 + \cdots + k_n \cdot n$, it will be preferred. We just have to remember that the order of the k_i is really irrelevant.

But when I is infinite, beware that $\mathbb{N}^{(I)}$ and the set $\mathbb{N}^I$ of ordered I-tuples are not isomorphic.

We are now ready to define polynomials.

30.2 Polynomials

We begin with polynomials in one variable.

Definition 30.2. Given a ring A, we define the set $\mathcal{P}_A(1)$ of *polynomials over A in one variable* as the set of functions $P\colon \mathbb{N} \to A$ such that $P(k) \neq 0$ for finitely many $k \in \mathbb{N}$. The polynomial such that $P(k) = 0$ for all $k \in \mathbb{N}$ is the *null (or zero) polynomial* and it is denoted by 0. We define addition of polynomials, multiplication by a scalar, and multiplication of polynomials, as follows: Given any three polynomials $P, Q, R \in \mathcal{P}_A(1)$, letting $a_k = P(k)$, $b_k = Q(k)$, and $c_k = R(k)$, for every $k \in \mathbb{N}$, we define $R = P + Q$ such that

$$c_k = a_k + b_k,$$

$R = \lambda P$ such that

$$c_k = \lambda a_k,$$

where $\lambda \in A$,

and $R = PQ$ such that

$$c_k = \sum_{i+j=k} a_i b_j.$$

We define the polynomial e_k such that $e_k(k) = 1$ and $e_k(i) = 0$ for $i \neq k$. We also denote e_0 by 1 when $k = 0$. Given a polynomial P, the $a_k = P(k) \in A$ are called the *coefficients of* P. If P is not the null polynomial, there is a greatest $n \geq 0$ such that $a_n \neq 0$ (and thus, $a_k = 0$ for all $k > n$) called the *degree of* P and denoted by $\deg(P)$. Then, P is written uniquely as

$$P = a_0e_0 + a_1e_1 + \cdots + a_ne_n.$$

When P is the null polynomial, we let $\deg(P) = -\infty$.

There is an injection of A into $\mathcal{P}_A(1)$ given by the map $a \mapsto a1$ (recall that 1 denotes e_0). There is also an injection of $\mathbb{N}$ into $\mathcal{P}_A(1)$ given by the map $k \mapsto e_k$. Observe that $e_k = e_1^k$ (with $e_1^0 = e_0 = 1$). In order to alleviate the notation, we often denote e_1 by X, and we call X a *variable (or indeterminate)*. Then, $e_k = e_1^k$ is denoted by X^k. Adopting this notation, given a nonnull polynomial P of degree n, if $P(k) = a_k$, P is denoted by

$$P = a_0 + a_1X + \cdots + a_nX^n,$$

or by

$$P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0,$$

if this is more convenient (the order of the terms does not matter anyway). Sometimes, it will also be convenient to write a polynomial as

$$P = a_0X^n + a_1X^{n-1} + \cdots + a_n.$$

The set $\mathcal{P}_A(1)$ is also denoted by $A[X]$ and a polynomial P may be denoted by $P(X)$. In denoting polynomials, we will use both upper-case and lower-case letters, usually, P, Q, R, S, p, q, r, s, but also f, g, h, etc., if needed (as long as no ambiguities arise).

Given a nonnull polynomial P of degree n, the nonnull coefficient a_n is called the *leading coefficient of* P. The coefficient a_0 is called the *constant term* of P. A polynomial of the form a_kX^k is called a *monomial*. We say that a_kX^k *occurs* in P if $a_k \neq 0$. A nonzero polynomial P of degree n is called a *monic polynomial (or unitary polynomial, or monic)* if $a_n = 1$, where a_n is its leading coefficient, and such a polynomial can be written as

$$P = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \qquad \text{or} \qquad P = X^n + a_1X^{n-1} + \cdots + a_n.$$

The choice of the variable X to denote e_1 is standard practice, but there is nothing special about X. We could have chosen Y, Z, or any other symbol, as long as no ambiguities arise.

Formally, the definition of $\mathcal{P}_A(1)$ has nothing to do with X. The reason for using X is simply convenience. Indeed, it is more convenient to write a polynomial as $P = a_0 + a_1X + \cdots + a_nX^n$ rather than as $P = a_0e_0 + a_1e_1 + \cdots + a_ne_n$.

We have the following simple but crucial proposition.

Proposition 30.1. *Given two nonnull polynomials $P(X) = a_0 + a_1X + \cdots + a_mX^m$ of degree m and $Q(X) = b_0 + b_1X + \cdots + b_nX^n$ of degree n, if either a_m or b_n is not a zero divisor, then $a_mb_n \neq 0$, and thus, $PQ \neq 0$ and*

$$\deg(PQ) = \deg(P) + \deg(Q).$$

In particular, if A is an integral domain, then $A[X]$ is an integral domain.

Proof. Since the coefficient of X^{m+n} in PQ is a_mb_n, and since we assumed that either a_m or a_n is not a zero divisor, we have $a_mb_n \neq 0$, and thus, $PQ \neq 0$ and

$$\deg(PQ) = \deg(P) + \deg(Q).$$

Then, it is obvious that $A[X]$ is an integral domain. □

It is easily verified that $A[X]$ is a commutative ring, with multiplicative identity $1X^0 = 1$. It is also easily verified that $A[X]$ satisfies all the conditions of Definition 3.1, but $A[X]$ is not a vector space, since A is not necessarily a field.

A structure satisfying the axioms of Definition 3.1 when K is a ring (and not necessarily a field) is called a *module*. Modules fail to have some of the nice properties that vector spaces have, and thus, they are harder to study. For example, there are modules that do not have a basis. We postpone the study of modules until Chapter 35.

However, when the ring A is a field, $A[X]$ is a vector space. But even when A is just a ring, the family of polynomials $(X^k)_{k\in\mathbb{N}}$ is a basis of $A[X]$, since every polynomial $P(X)$ can be written in a unique way as $P(X) = a_0 + a_1X + \cdots + a_nX^n$ (with $P(X) = 0$ when $P(X)$ is the null polynomial). Thus, $A[X]$ is a free module.

Next, we want to define the notion of evaluating a polynomial $P(X)$ at some $\alpha \in A$. For this, we need a proposition.

Proposition 30.2. *Let A, B be two rings and let $h\colon A \to B$ be a ring homomorphism. For any $\beta \in B$, there is a unique ring homomorphism $\varphi\colon A[X] \to B$ extending h such that $\varphi(X) = \beta$, as in the following diagram (where we denote by $h+\beta$ the map $h+\beta\colon A\cup\{X\} \to B$ such that $(h+\beta)(a) = h(a)$ for all $a \in A$ and $(h+\beta)(X) = \beta$):*

$$\begin{tikzcd}
A \cup \{X\} \arrow[r, "\iota"] \arrow[dr, "h+\beta"'] & A[X] \arrow[d, "\varphi"] \\
 & B
\end{tikzcd}$$

Proof. Let $\varphi(0) = 0$, and for every nonull polynomial $P(X) = a_0 + a_1X + \cdots + a_nX^n$, let

$$\varphi(P(X)) = h(a_0) + h(a_1)\beta + \cdots + h(a_n)\beta^n.$$

It is easily verified that φ is the unique homomorphism $\varphi\colon A[X] \to B$ extending h such that $\varphi(X) = \beta$. □

Taking $A = B$ in Proposition 30.2 and $h\colon A \to A$ the identity, for every $\beta \in A$, there is a unique homomorphism $\varphi_\beta\colon A[X] \to A$ such that $\varphi_\beta(X) = \beta$, and for every polynomial $P(X)$, we write $\varphi_\beta(P(X))$ as $P(\beta)$ and we call $P(\beta)$ the *value of* $P(X)$ *at* $X = \beta$. Thus, we can define a function $P_A\colon A \to A$ such that $P_A(\beta) = P(\beta)$, for all $\beta \in A$. This function is called the *polynomial function induced by* P.

More generally, P_B can be defined for any (commutative) ring B such that $A \subseteq B$. In general, it is possible that $P_A = Q_A$ for distinct polynomials P, Q. We will see shortly conditions for which the map $P \mapsto P_A$ is injective. In particular, this is true for $A = \mathbb{R}$ (in general, any infinite integral domain). We now define polynomials in n variables.

Definition 30.3. Given $n \geq 1$ and a ring A, the set $\mathcal{P}_A(n)$ of *polynomials over* A *in* n *variables* is the set of functions $P\colon \mathbb{N}^{(n)} \to A$ such that $P(k_1, \ldots, k_n) \neq 0$ for finitely many $(k_1, \ldots, k_n) \in \mathbb{N}^{(n)}$. The polynomial such that $P(k_1, \ldots, k_n) = 0$ for all $(k_1, \ldots, k_n)$ is the *null (or zero) polynomial* and it is denoted by 0. We define addition of polynomials, multiplication by a scalar, and multiplication of polynomials, as follows: Given any three polynomials $P, Q, R \in \mathcal{P}_A(n)$, letting $a_{(k_1,\ldots,k_n)} = P(k_1, \ldots, k_n)$, $b_{(k_1,\ldots,k_n)} = Q(k_1, \ldots, k_n)$, $c_{(k_1,\ldots,k_n)} = R(k_1, \ldots, k_n)$, for every $(k_1, \ldots, k_n) \in \mathbb{N}^{(n)}$, we define $R = P + Q$ such that

$$c_{(k_1,\ldots,k_n)} = a_{(k_1,\ldots,k_n)} + b_{(k_1,\ldots,k_n)},$$

$R = \lambda P$, where $\lambda \in A$, such that

$$c_{(k_1,\ldots,k_n)} = \lambda a_{(k_1,\ldots,k_n)},$$

and $R = PQ$, such that

$$c_{(k_1,\ldots,k_n)} = \sum_{(i_1,\ldots,i_n)+(j_1,\ldots,j_n)=(k_1,\ldots,k_n)} a_{(i_1,\ldots,i_n)} b_{(j_1,\ldots,j_n)}.$$

For every $(k_1, \ldots, k_n) \in \mathbb{N}^{(n)}$, we let $e_{(k_1,\ldots,k_n)}$ be the polynomial such that

$$e_{(k_1,\ldots,k_n)}(k_1, \ldots, k_n) = 1 \quad \text{and} \quad e_{(k_1,\ldots,k_n)}(h_1, \ldots, h_n) = 0,$$

for $(h_1, \ldots, h_n) \neq (k_1, \ldots, k_n)$. We also denote $e_{(0,\ldots,0)}$ by 1. Given a polynomial P, the $a_{(k_1,\ldots,k_n)} = P(k_1, \ldots, k_n) \in A$, are called the *coefficients of* P. If P is not the null polynomial, there is a greatest $d \geq 0$ such that $a_{(k_1,\ldots,k_n)} \neq 0$ for some $(k_1, \ldots, k_n) \in \mathbb{N}^{(n)}$, with $d = k_1 + \cdots + k_n$, called the *total degree of* P and denoted by $\deg(P)$. Then, P is written uniquely as

$$P = \sum_{(k_1,\ldots,k_n)\in\mathbb{N}^{(n)}} a_{(k_1,\ldots,k_n)} e_{(k_1,\ldots,k_n)}.$$

When P is the null polynomial, we let $\deg(P) = -\infty$.

There is an injection of A into $\mathcal{P}_A(n)$ given by the map $a \mapsto a1$ (where 1 denotes $e_{(0,\ldots,0)}$). There is also an injection of $\mathbb{N}^{(n)}$ into $\mathcal{P}_A(n)$ given by the map $(h_1, \ldots, h_n) \mapsto e_{(h_1,\ldots,h_n)}$. Note that $e_{(h_1,\ldots,h_n)} e_{(k_1,\ldots,k_n)} = e_{(h_1+k_1,\ldots,h_n+k_n)}$. In order to alleviate the notation, let $X_1, \ldots, X_n$ be n distinct variables and denote $e_{(0,\ldots,0,1,0\ldots,0)}$, where 1 occurs in the position i, by X_i (where $1 \leq i \leq n$). With this convention, in view of $e_{(h_1,\ldots,h_n)} e_{(k_1,\ldots,k_n)} = e_{(h_1+k_1,\ldots,h_n+k_n)}$, the polynomial $e_{(k_1,\ldots,k_n)}$ is denoted by $X_1^{k_1} \cdots X_n^{k_n}$ (with $e_{(0,\ldots,0)} = X_1^0 \cdots X_n^0 = 1$) and it is called a *primitive monomial*. Then, P is also written as

$$P = \sum_{(k_1,\ldots,k_n)\in\mathbb{N}^{(n)}} a_{(k_1,\ldots,k_n)} X_1^{k_1} \cdots X_n^{k_n}.$$

We also denote $\mathcal{P}_A(n)$ by $A[X_1, \ldots, X_n]$. A polynomial $P \in A[X_1, \ldots, X_n]$ is also denoted by $P(X_1, \ldots, X_n)$.

As in the case $n = 1$, there is nothing special about the choice of $X_1, \ldots, X_n$ as variables (or indeterminates). It is just a convenience. After all, the construction of $\mathcal{P}_A(n)$ has nothing to do with $X_1, \ldots, X_n$.

Given a nonnull polynomial P of degree d, the nonnull coefficients $a_{(k_1,\ldots,k_n)} \neq 0$ such that $d = k_1 + \cdots + k_n$ are called the *leading coefficients of* P. A polynomial of the form $a_{(k_1,\ldots,k_n)} X_1^{k_1} \cdots X_n^{k_n}$ is called a *monomial*. Note that $\deg(a_{(k_1,\ldots,k_n)} X_1^{k_1} \cdots X_n^{k_n}) = k_1 + \cdots + k_n$. Given a polynomial

$$P = \sum_{(k_1,\ldots,k_n)\in\mathbb{N}^{(n)}} a_{(k_1,\ldots,k_n)} X_1^{k_1} \cdots X_n^{k_n},$$

a monomial $a_{(k_1,\ldots,k_n)} X_1^{k_1} \cdots X_n^{k_n}$ *occurs in the polynomial* P if $a_{(k_1,\ldots,k_n)} \neq 0$.

A polynomial

$$P = \sum_{(k_1,\ldots,k_n)\in\mathbb{N}^{(n)}} a_{(k_1,\ldots,k_n)} X_1^{k_1} \cdots X_n^{k_n}$$

is *homogeneous of degree* d if

$$\deg(X_1^{k_1} \cdots X_n^{k_n}) = d,$$

for every monomial $a_{(k_1,\ldots,k_n)} X_1^{k_1} \cdots X_n^{k_n}$ occurring in P. If P is a polynomial of total degree d, it is clear that P can be written uniquely as

$$P = P^{(0)} + P^{(1)} + \cdots + P^{(d)},$$

where $P^{(i)}$ is the sum of all monomials of degree i occurring in P, where $0 \leq i \leq d$.

It is easily verified that $A[X_1, \ldots, X_n]$ is a commutative ring, with multiplicative identity $1X_1^0 \cdots X_n^0 = 1$. It is also easily verified that $A[X]$ is a module. When A is a field, $A[X]$ is a vector space.

Even when A is just a ring, the family of polynomials

$$(X_1^{k_1} \cdots X_n^{k_n})_{(k_1,\ldots,k_n)\in\mathbb{N}^{(n)}}$$

is a basis of $A[X_1, \ldots, X_n]$, since every polynomial $P(X_1, \ldots, X_n)$ can be written in a unique way as

$$P(X_1, \ldots, X_n) = \sum_{(k_1,\ldots,k_n)\in \mathbb{N}^{(n)}} a_{(k_1,\ldots,k_n)} X_1^{k_1} \cdots X_n^{k_n}.$$

Thus, $A[X_1, \ldots, X_n]$ is a free module.

Remark: The construction of Definition 30.3 can be immediately extended to an arbitrary set I, and not just $I = \{1, \ldots, n\}$. It can also be applied to monoids more general that $\mathbb{N}^{(I)}$.

Proposition 30.2 is generalized as follows.

Proposition 30.3. *Let A, B be two rings and let $h\colon A \to B$ be a ring homomorphism. For any $\beta = (\beta_1, \ldots, \beta_n) \in B^n$, there is a unique ring homomorphism $\varphi\colon A[X_1, \ldots, X_n] \to B$ extending h such that $\varphi(X_i) = \beta_i$, $1 \leq i \leq n$, as in the following diagram (where we denote by $h + \beta$ the map $h + \beta\colon A \cup \{X_1, \ldots, X_n\} \to B$ such that $(h + \beta)(a) = h(a)$ for all $a \in A$ and $(h + \beta)(X_i) = \beta_i$, $1 \leq i \leq n$):*

$$\begin{tikzcd}
A \cup \{X_1, \ldots, X_n\} \arrow[r, "\iota"] \arrow[dr, "h+\beta"'] & A[X_1, \ldots, X_n] \arrow[d, "\varphi"] \\
& B
\end{tikzcd}$$

Proof. Let $\varphi(0) = 0$, and for every nonnull polynomial

$$P(X_1, \ldots, X_n) = \sum_{(k_1,\ldots,k_n)\in \mathbb{N}^{(n)}} a_{(k_1,\ldots,k_n)} X_1^{k_1} \cdots X_n^{k_n},$$

let

$$\varphi(P(X_1, \ldots, X_n)) = \sum h(a_{(k_1,\ldots,k_n)}) \beta_1^{k_1} \cdots \beta_n^{k_n}.$$

It is easily verified that φ is the unique homomorphism $\varphi\colon A[X_1, \ldots, X_n] \to B$ extending h such that $\varphi(X_i) = \beta_i$. □

Taking $A = B$ in Proposition 30.3 and $h\colon A \to A$ the identity, for every $\beta_1, \ldots, \beta_n \in A$, there is a unique homomorphism $\varphi\colon A[X_1, \ldots, X_n] \to A$ such that $\varphi(X_i) = \beta_i$, and for every polynomial $P(X_1, \ldots, X_n)$, we write $\varphi(P(X_1, \ldots, X_n))$ as $P(\beta_1, \ldots, \beta_n)$ and we call $P(\beta_1, \ldots, \beta_n)$ the *value of* $P(X_1, \ldots, X_n)$ *at* $X_1 = \beta_1, \ldots, X_n = \beta_n$. Thus, we can define a function $P_A\colon A^n \to A$ such that $P_A(\beta_1, \ldots, \beta_n) = P(\beta_1, \ldots, \beta_n)$, for all $\beta_1, \ldots, \beta_n \in A$. This function is called the *polynomial function induced by* P.

More generally, P_B can be defined for any (commutative) ring B such that $A \subseteq B$. As in the case of a single variable, it is possible that $P_A = Q_A$ for distinct polynomials P, Q. We will see shortly that the map $P \mapsto P_A$ is injective when $A = \mathbb{R}$ (in general, any infinite integral domain).

Given any nonnull polynomial $P(X_1, \ldots, X_n) = \sum_{(k_1,\ldots,k_n)\in\mathbb{N}^{(n)}} a_{(k_1,\ldots,k_n)} X_1^{k_1} \cdots X_n^{k_n}$ in $A[X_1, \ldots, X_n]$, where $n \geq 2$, $P(X_1, \ldots, X_n)$ can be uniquely written as

$$P(X_1, \ldots, X_n) = \sum Q_{k_n}(X_1, \ldots, X_{n-1}) X_n^{k_n},$$

where each polynomial $Q_{k_n}(X_1, \ldots, X_{n-1})$ is in $A[X_1, \ldots, X_{n-1}]$. Even if A is a field, $A[X_1, \ldots, X_{n-1}]$ is not a field, which confirms that it is useful (and necessary!) to consider polynomials over rings that are not necessarily fields.

It is not difficult to show that $A[X_1, \ldots, X_n]$ and $A[X_1, \ldots, X_{n-1}][X_n]$ are isomorphic rings. This way, it is often possible to prove properties of polynomials in several variables $X_1, \ldots, X_n$, by induction on the number n of variables. For example, given two nonnull polynomials $P(X_1, \ldots, X_n)$ of total degree p and $Q(X_1, \ldots, X_n)$ of total degree q, since we assumed that A is an integral domain, we can prove that

$$\deg(PQ) = \deg(P) + \deg(Q),$$

and that $A[X_1, \ldots, X_n]$ is an integral domain.

Next, we will consider the division of polynomials (in one variable).

30.3 Euclidean Division of Polynomials

We know that every natural number $n \geq 2$ can be written uniquely as a product of powers of prime numbers and that prime numbers play a very important role in arithmetic. It would be nice if every polynomial could be expressed (uniquely) as a product of "irreducible" factors. This is indeed the case for polynomials over a field. The fact that there is a division algorithm for the natural numbers is essential for obtaining many of the arithmetical properties of the natural numbers. As we shall see next, there is also a division algorithm for polynomials in $A[X]$, when A is a field.

Proposition 30.4. *Let A be a ring, let $f(X), g(X) \in A[X]$ be two polynomials of degree $m = \deg(f)$ and $n = \deg(g)$ with $f(X) \neq 0$, and assume that the leading coefficient a_m of $f(X)$ is invertible. Then, there exist unique polynomials $q(X)$ and $r(X)$ in $A[X]$ such that*

$$g = fq + r \quad \textit{and} \quad \deg(r) < \deg(f) = m.$$

Proof. We first prove the existence of q and r. Let

$$f = a_m X^m + a_{m-1} X^{m-1} + \cdots + a_0,$$

and

$$g = b_n X^n + b_{n-1} X^{n-1} + \cdots + b_0.$$

If $n < m$, then let $q = 0$ and $r = g$. Since $\deg(g) < \deg(f)$ and $r = g$, we have $\deg(r) < \deg(f)$.

If $n \geq m$, we proceed by induction on n. If $n = 0$, then $g = b_0$, $m = 0$, $f = a_0 \neq 0$, and we let $q = a_0^{-1} b_0$ and $r = 0$. Since $\deg(r) = \deg(0) = -\infty$ and $\deg(f) = \deg(a_0) = 0$ because $a_0 \neq 0$, we have $\deg(r) < \deg(f)$.

If $n \geq 1$, since $n \geq m$, note that

$$\begin{aligned} g_1(X) &= g(X) - b_n a_m^{-1} X^{n-m} f(X) \\ &= b_n X^n + b_{n-1} X^{n-1} + \cdots + b_0 - b_n a_m^{-1} X^{n-m}(a_m X^m + a_{m-1} X^{m-1} + \cdots + a_0) \end{aligned}$$

is a polynomial of degree $\deg(g_1) < n$, since the terms $b_n X^n$ and $b_n a_m^{-1} X^{n-m} a_m X^m$ of degree n cancel out. Now, since $\deg(g_1) < n$, by the induction hypothesis, we can find q_1 and r such that

$$g_1 = f q_1 + r \quad \text{and} \quad \deg(r) < \deg(f) = m,$$

and thus,

$$g_1(X) = g(X) - b_n a_m^{-1} X^{n-m} f(X) = f(X) q_1(X) + r(X),$$

from which, letting $q(X) = b_n a_m^{-1} X^{n-m} + q_1(X)$, we get

$$g = fq + r \quad \text{and} \quad \deg(r) < m = \deg(f).$$

We now prove uniqueness. If

$$g = f q_1 + r_1 = f q_2 + r_2,$$

with $\deg(r_1) < \deg(f)$ and $\deg(r_2) < \deg(f)$, we get

$$f(q_1 - q_2) = r_2 - r_1.$$

If $q_2 - q_1 \neq 0$, since the leading coefficient a_m of f is invertible, by Proposition 30.1, we have

$$\deg(r_2 - r_1) = \deg(f(q_1 - q_2)) = \deg(f) + \deg(q_2 - q_1),$$

and so, $\deg(r_2 - r_1) \geq \deg(f)$, which contradicts the fact that $\deg(r_1) < \deg(f)$ and $\deg(r_2) < \deg(f)$. Thus, $q_1 = q_2$, and then also $r_1 = r_2$. □

It should be noted that the proof of Proposition 30.4 actually provides an algorithm for finding the *quotient* q and the *remainder* r of the division of g by f. This algorithm is called the *Euclidean algorithm, or division algorithm.* Note that the division of g by f is always possible when f is a monic polynomial, since 1 is invertible. Also, when A is a field, $a_m \neq 0$ is always invertible, and thus, the division can always be performed. We say that f *divides* g when $r = 0$ in the result of the division $g = fq + r$. We now draw some important consequences of the existence of the Euclidean algorithm.

30.4 Ideals, PID's, and Greatest Common Divisors

First, we introduce the fundamental concept of an ideal.

Definition 30.4. Given a ring A, an *ideal of A* is any nonempty subset $\mathfrak{I}$ of A satisfying the following two properties:

(ID1) If $a, b \in \mathfrak{I}$, then $b - a \in \mathfrak{I}$.

(ID2) If $a \in \mathfrak{I}$, then $ax \in \mathfrak{I}$ for every $x \in A$.

An ideal $\mathfrak{I}$ is a *principal ideal* if there is some $a \in \mathfrak{I}$, called a *generator*, such that

$$\mathfrak{I} = \{ax \mid x \in A\}.$$

The equality $\mathfrak{I} = \{ax \mid x \in A\}$ is also written as $\mathfrak{I} = aA$ or as $\mathfrak{I} = (a)$. The ideal $\mathfrak{I} = (0) = \{0\}$ is called the *null ideal* (or *zero ideal*).

An ideal $\mathfrak{I}$ is a *maximal ideal* if $\mathfrak{I} \neq A$ and for every ideal $\mathfrak{J} \neq A$, if $\mathfrak{I} \subseteq \mathfrak{J}$, then $\mathfrak{J} = \mathfrak{I}$. An ideal $\mathfrak{I}$ is a *prime ideal* if $\mathfrak{I} \neq A$ and if $ab \in \mathfrak{I}$, then $a \in \mathfrak{I}$ or $b \in \mathfrak{I}$, for all $a, b \in A$. Equivalently, $\mathfrak{I}$ is a prime ideal if $\mathfrak{I} \neq A$ and if $a, b \in A - \mathfrak{I}$, then $ab \in A - \mathfrak{I}$, for all $a, b \in A$. In other words, $A - \mathfrak{I}$ is closed under multiplication and $1 \in A - \mathfrak{I}$.

Note that if $\mathfrak{I}$ is an ideal, then $\mathfrak{I} = A$ iff $1 \in \mathfrak{I}$. Since by definition, an ideal $\mathfrak{I}$ is nonempty, there is some $a \in \mathfrak{I}$, and by (ID1) we get $0 = a - a \in \mathfrak{I}$. Then, for every $a \in \mathfrak{I}$, since $0 \in \mathfrak{I}$, by (ID1) we get $-a \in \mathfrak{I}$. Thus, an ideal is an additive subgroup of A. Because of (ID2), an ideal is also a subring.

Observe that if A is a field, then A only has two ideals, namely, the trivial ideal (0) and A itself. Indeed, if $\mathfrak{I} \neq (0)$, because every nonnull element has an inverse, then $1 \in \mathfrak{I}$, and thus, $\mathfrak{I} = A$.

Definition 30.5. Given a ring A, for any two elements $a, b \in A$ we say that b *is a multiple of a and that a divides b* if $b = ac$ for some $c \in A$; this is usually denoted by $a \mid b$.

Note that the principal ideal (a) is the set of all multiples of a, and that a divides b iff b is a multiple of a iff $b \in (a)$ iff $(b) \subseteq (a)$.

Note that every $a \in A$ divides 0. However, it is customary to say that a is a *zero divisor* iff $ac = 0$ for some $c \neq 0$. With this convention, 0 is a zero divisor unless $A = \{0\}$ (the trivial ring), and A is an integral domain iff 0 is the only zero divisor in A.

Given $a, b \in A$ with $a, b \neq 0$, if $(a) = (b)$ then there exist $c, d \in A$ such that $a = bc$ and $b = ad$. From this, we get $a = adc$ and $b = bcd$, that is, $a(1 - dc) = 0$ and $b(1 - cd) = 0$. If A is an integral domain, we get $dc = 1$ and $cd = 1$, that is, c is invertible with inverse d. Thus, when A is an integral domain, we have $b = ad$, with d invertible. The converse is obvious, if $b = ad$ with d invertible, then $(a) = (b)$.

It is worth recording this fact as the following proposition.

Proposition 30.5. *If A is an integral domain, for any $a, b \in A$ with $a, b \neq 0$, we have $(a) = (b)$ iff there exists some invertible $d \in A$ such that $b = ad$.*

An invertible element $u \in A$ is also called a *unit*.

Given two ideals $\mathfrak{I}$ and $\mathfrak{J}$, their sum

$$\mathfrak{I} + \mathfrak{J} = \{a + b \mid a \in \mathfrak{I},\ b \in \mathfrak{J}\}$$

is clearly an ideal. Given any nonempty subset J of A, the set

$$\{a_1x_1 + \cdots + a_nx_n \mid x_1, \ldots, x_n \in A,\, a_1, \ldots, a_n \in J,\, n \geq 1\}$$

is easily seen to be an ideal, and in fact, it is the smallest ideal containing J. It is usually denoted by (J).

Ideals play a very important role in the study of rings. They tend to show up everywhere. For example, they arise naturally from homomorphisms.

Proposition 30.6. *Given any ring homomorphism $h\colon A \to B$, the kernel* $\mathrm{Ker}\, h = \{a \in A \mid h(a) = 0\}$ *of h is an ideal.*

Proof. Given $a, b \in A$, we have $a, b \in \mathrm{Ker}\, h$ iff $h(a) = h(b) = 0$, and since h is a homomorphism, we get

$$h(b - a) = h(b) - h(a) = 0,$$

and

$$h(ax) = h(a)h(x) = 0$$

for all $x \in A$, which shows that $\mathrm{Ker}\, h$ is an ideal. □

There is a sort of converse property. Given a ring A and an ideal $\mathfrak{I} \subseteq A$, we can define the quotient ring $A/\mathfrak{I}$, and there is a surjective homomorphism $\pi\colon A \to A/\mathfrak{I}$ whose kernel is precisely $\mathfrak{I}$.

Proposition 30.7. *Given any ring A and any ideal $\mathfrak{I} \subseteq A$, the equivalence relation $\equiv_{\mathfrak{I}}$ defined by $a \equiv_{\mathfrak{I}} b$ iff $b - a \in \mathfrak{I}$ is a congruence, which means that if $a_1 \equiv_{\mathfrak{I}} b_1$ and $a_2 \equiv_{\mathfrak{I}} b_2$, then*

1. *$a_1 + a_2 \equiv_{\mathfrak{I}} b_1 + b_2$, and*

2. *$a_1a_2 \equiv_{\mathfrak{I}} b_1b_2$.*

Then, the set $A/\mathfrak{I}$ of equivalence classes modulo $\mathfrak{I}$ is a ring under the operations

$$\begin{aligned} [a] + [b] &= [a + b] \\ [a][b] &= [ab]. \end{aligned}$$

The map $\pi\colon A \to A/\mathfrak{I}$ such that $\pi(a) = [a]$ is a surjective homomorphism whose kernel is precisely $\mathfrak{I}$.

Proof. Everything is straightforward. For example, if $a_1 \equiv_{\mathfrak{I}} b_1$ and $a_2 \equiv_{\mathfrak{I}} b_2$, then $b_1 - a_1 \in \mathfrak{I}$ and $b_2 - a_2 \in \mathfrak{I}$. Since $\mathfrak{I}$ is an ideal, we get

$$(b_1 - a_1)b_2 = b_1b_2 - a_1b_2 \in \mathfrak{I}$$

and

$$(b_2 - a_2)a_1 = a_1b_2 - a_1a_2 \in \mathfrak{I}.$$

Since $\mathfrak{I}$ is an ideal, and thus, an additive group, we get

$$b_1b_2 - a_1a_2 \in \mathfrak{I},$$

i.e., $a_1a_2 \equiv_{\mathfrak{I}} b_1b_2$. The equality $\mathrm{Ker}\,\pi = \mathfrak{I}$ holds because $\mathfrak{I}$ is an ideal. □

Example 30.1.

1. In the ring $\mathbb{Z}$, for every $p \in \mathbb{Z}$, the subroup $p\mathbb{Z}$ is an ideal, and $\mathbb{Z}/p\mathbb{Z}$ is a ring, the ring of residues modulo p. This ring is a field iff p is a prime number.

2. The quotient of the polynomial ring $\mathbb{R}[X]$ by a prime ideal $\mathfrak{I}$ is an integral domain.

3. The quotient of the polynomial ring $\mathbb{R}[X]$ by a maximal ideal $\mathfrak{I}$ is a field. For example, if $\mathfrak{I} = (X^2 + 1)$, the principal ideal generated by $X^2 + 1$ (which is indeed a maximal ideal since $X^2 + 1$ has no real roots), then $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$.

The following proposition yields a characterization of prime ideals and maximal ideals in terms of quotients.

Proposition 30.8. *Given a ring A, for any ideal $\mathfrak{I} \subseteq A$, the following properties hold.*

(1) The ideal $\mathfrak{I}$ is a prime ideal iff $A/\mathfrak{I}$ is an integral domain.

(2) The ideal $\mathfrak{I}$ is a maximal ideal iff $A/\mathfrak{I}$ is a field.

Proof. (1) Assume that $\mathfrak{I}$ is a prime ideal. Since $\mathfrak{I}$ is prime, $\mathfrak{I} \neq A$, and thus, $A/\mathfrak{I}$ is not the trivial ring (0). If $[a][b] = 0$, since $[a][b] = [ab]$, we have $ab \in \mathfrak{I}$, and since $\mathfrak{I}$ is prime, then either $a \in \mathfrak{I}$ or $b \in \mathfrak{I}$, so that either $[a] = 0$ or $[b] = 0$. Thus, $A/\mathfrak{I}$ is an integral domain.

Conversely, assume that $A/\mathfrak{I}$ is an integral domain. Since $A/\mathfrak{I}$ is not the trivial ring, $\mathfrak{I} \neq A$. Assume that $ab \in \mathfrak{I}$. Then, we have

$$\pi(ab) = \pi(a)\pi(b) = 0,$$

which implies that either $\pi(a) = 0$ or $\pi(b) = 0$, since $A/\mathfrak{I}$ is an integral domain (where $\pi\colon A \to A/\mathfrak{I}$ is the quotient map). Thus, either $a \in \mathfrak{I}$ or $b \in \mathfrak{I}$, and $\mathfrak{I}$ is a prime ideal.

(2) Assume that $\mathfrak{I}$ is a maximal ideal. As in (1), $A/\mathfrak{I}$ is not the trivial ring (0). Let $[a] \neq 0$ in $A/\mathfrak{I}$. We need to prove that $[a]$ has a multiplicative inverse. Since $[a] \neq 0$, we have $a \notin \mathfrak{I}$. Let $\mathfrak{I}_a$ be the ideal generated by $\mathfrak{I}$ and a. We have

$$\mathfrak{I} \subseteq \mathfrak{I}_a \quad \text{and} \quad \mathfrak{I} \neq \mathfrak{I}_a,$$

since $a \notin \mathfrak{I}$, and since $\mathfrak{I}$ is maximal, this implies that

$$\mathfrak{I}_a = A.$$

However, we know that

$$\mathfrak{I}_a = \{ax + h \mid x \in A,\, h \in \mathfrak{I}\},$$

and thus, there is some $x \in A$ so that

$$ax + h = 1,$$

which proves that $[a][x] = [1]$, as desired.

Conversely, assume that $A/\mathfrak{I}$ is a field. Again, since $A/\mathfrak{I}$ is not the trivial ring, $\mathfrak{I} \neq A$. Let $\mathfrak{J}$ be any proper ideal such that $\mathfrak{I} \subseteq \mathfrak{J}$, and assume that $\mathfrak{I} \neq \mathfrak{J}$. Thus, there is some $j \in \mathfrak{J} - \mathfrak{I}$, and since $\mathrm{Ker}\,\pi = \mathfrak{I}$, we have $\pi(j) \neq 0$. Since $A/\mathfrak{I}$ is a field and π is surjective, there is some $k \in A$ so that $\pi(j)\pi(k) = 1$, which implies that

$$jk - 1 = i$$

for some $i \in \mathfrak{I}$, and since $\mathfrak{I} \subset \mathfrak{J}$ and $\mathfrak{J}$ is an ideal, it follows that $1 = jk - i \in \mathfrak{J}$, showing that $\mathfrak{J} = A$, a contradiction. Therefore, $\mathfrak{I} = \mathfrak{J}$, and $\mathfrak{I}$ is a maximal ideal. □

As a corollary, we obtain the following useful result. It emphasizes the importance of maximal ideals.

Corollary 30.9. *Given any ring A, every maximal ideal $\mathfrak{I}$ in A is a prime ideal.*

Proof. If $\mathfrak{I}$ is a maximal ideal, then, by Proposition 30.8, the quotient ring $A/\mathfrak{I}$ is a field. However, a field is an integral domain, and by Proposition 30.8 (again), $\mathfrak{I}$ is a prime ideal. □

Observe that a ring A is an integral domain iff (0) is a prime ideal. This is an example of a prime ideal which is not a maximal ideal, as immediately seen in $A = \mathbb{Z}$, where (p) is a maximal ideal for every prime number p.

A less obvious example of a prime ideal which is not a maximal ideal is the ideal (X) in the ring of polynomials $\mathbb{Z}[X]$. Indeed, $(X, 2)$ is also a prime ideal, but (X) is properly contained in $(X, 2)$. The ideal (X) is the set of all polynomials of the form $XQ(X)$ for any $Q(X) \in \mathbb{Z}[X]$, in other words the set of all polynomials in $\mathbb{Z}[X]$ with constant term equal to 0, and the ideal $(X, 2)$ is the set of all polynomials of the form

$$XQ_1(X) + 2Q_2(X), \quad Q_1(X), Q_2(X) \in \mathbb{Z}[X],$$

which is just the set of all polynomials in $\mathbb{Z}[X]$ whose constant term is of the form $2c$ for some $c \in \mathbb{Z}$. The ideal (X) is indeed properly contained in the ideal $(X, 2)$. If $P(X)Q(X) \in (X, 2)$, let a be the constant term in $P(X)$ and let b be the constant term in $Q(X)$. Since $P(X)Q(X) \in (X, 2)$, we must have $ab = 2c$ for some $c \in \mathbb{Z}$, and since 2 is prime, either a is divisible by 2 or b is divisible by 2. It follows that either $P(X) \in (X, 2)$ or $Q(X) \in (X, 2)$, which shows that $(X, 2)$ is a prime ideal.

Definition 30.6. An integral domain in which every ideal is a principal ideal is called a *principal ring or principal ideal domain*, for short, a *PID*.

The ring $\mathbb{Z}$ is a PID. This is a consequence of the existence of a (Euclidean) division algorithm. As we shall see next, when K is a field, the ring $K[X]$ is also a principal ring.

However, when $n \geq 2$, the ring $K[X_1, \ldots, X_n]$ is not principal. For example, in the ring $K[X, Y]$, the ideal (X, Y) generated by X and Y is not principal. First, since (X, Y) is the set of all polynomials of the form $Xq_1 + Yq_2$, where $q_1, q_2 \in K[X, Y]$, except when $Xq_1 + Yq_2 = 0$, we have $\deg(Xq_1 + Yq_2) \geq 1$. Thus, $1 \notin (X, Y)$. Now if there was some $p \in K[X, Y]$ such that $(X, Y) = (p)$, since $1 \notin (X, Y)$, we must have $\deg(p) \geq 1$. But we would also have $X = pq_1$ and $Y = pq_2$, for some $q_1, q_2 \in K[X, Y]$. Since $\deg(X) = \deg(Y) = 1$, this is impossible.

Even though $K[X, Y]$ is not a principal ring, a suitable version of unique factorization in terms of irreducible factors holds. The ring $K[X, Y]$ (and more generally $K[X_1, \ldots, X_n]$) is what is called a *unique factorization domain*, for short, UFD, or a *factorial ring*.

From this point until Definition 30.11, we consider polynomials in one variable over a field K.

Remark: Although we already proved part (1) of Proposition 30.10 in a more general situation above, we reprove it in the special case of polynomials. This may offend the purists, but most readers will probably not mind.

Proposition 30.10. *Let K be a field. The following properties hold:*

(1) For any two nonzero polynomials $f, g \in K[X]$, $(f) = (g)$ iff there is some $\lambda \neq 0$ in K such that $g = \lambda f$.

(2) For every nonnull ideal $\mathfrak{I}$ in $K[X]$, there is a unique monic polynomial $f \in K[X]$ such that $\mathfrak{I} = (f)$.

Proof. (1) If $(f) = (g)$, there are some nonzero polynomials $q_1, q_2 \in K[X]$ such that $g = fq_1$ and $f = gq_2$. Thus, we have $f = fq_1q_2$, which implies $f(1 - q_1q_2) = 0$. Since K is a field, by Proposition 30.1, $K[X]$ has no zero divisor, and since we assumed $f \neq 0$, we must have $q_1q_2 = 1$. However, if either q_1 or q_2 is not a constant, by Proposition 30.1 again, $\deg(q_1q_2) = \deg(q_1) + \deg(q_2) \geq 1$, contradicting $q_1q_2 = 1$, since $\deg(1) = 0$. Thus, both $q_1, q_2 \in K - \{0\}$, and (1) holds with $\lambda = q_1$. In the other direction, it is obvious that $g = \lambda f$ implies that $(f) = (g)$.

(2) Since we are assuming that $\mathfrak{I}$ is not the null ideal, there is some polynomial of smallest degree in $\mathfrak{I}$, and since K is a field, by suitable multiplication by a scalar, we can make sure that this polynomial is monic. Thus, let f be a monic polynomial of smallest degree in $\mathfrak{I}$. By (ID2), it is clear that $(f) \subseteq \mathfrak{I}$. Now, let $g \in \mathfrak{I}$. Using the Euclidean algorithm, there exist unique $q, r \in K[X]$ such that

$$g = qf + r \quad \text{and} \quad \deg(r) < \deg(f).$$

If $r \neq 0$, there is some $\lambda \neq 0$ in K such that λr is a monic polynomial, and since $\lambda r = \lambda g - \lambda q f$, with $f, g \in \mathfrak{I}$, by (ID1) and (ID2), we have $\lambda r \in \mathfrak{I}$, where $\deg(\lambda r) < \deg(f)$ and λr is a monic polynomial, contradicting the minimality of the degree of f. Thus, $r = 0$, and $g \in (f)$. The uniqueness of the monic polynomial f follows from (1). □

Proposition 30.10 shows that $K[X]$ is a principal ring when K is a field.

We now investigate the existence of a greatest common divisor (gcd) for two nonzero polynomials. Given any two nonzero polynomials $f, g \in K[X]$, recall that f divides g if $g = fq$ for some $q \in K[X]$.

Definition 30.7. Given any two nonzero polynomials $f, g \in K[X]$, a polynomial $d \in K[X]$ is a *greatest common divisor of f and g* (for short, a *gcd of f and g*) if d divides f and g and whenever $h \in K[X]$ divides f and g, then h divides d. We say that f and g are *relatively prime* if 1 is a gcd of f and g.

Note that f and g are relatively prime iff all of their gcd's are constants (scalars in K), or equivalently, if f, g have no divisor q of degree $\deg(q) \geq 1$.

In particular, note that f and g are relatively prime when f is a nonzero constant polynomial (a scalar $\lambda \neq 0$ in K) and g is any nonzero polynomial.

We can characterize gcd's of polynomials as follows.

Proposition 30.11. *Let K be a field and let $f, g \in K[X]$ be any two nonzero polynomials. For every polynomial $d \in K[X]$, the following properties are equivalent:*

(1) The polynomial d is a gcd of f and g.

(2) The polynomial d divides f and g and there exist $u, v \in K[X]$ such that

$$d = uf + vg.$$

(3) The ideals $(f), (g)$, and (d) satisfy the equation

$$(d) = (f) + (g).$$

In addition, $d \neq 0$, and d is unique up to multiplication by a nonzero scalar in K.

Proof. Given any two nonzero polynomials $u, v \in K[X]$, observe that u divides v iff $(v) \subseteq (u)$. Now, (2) can be restated as $(f) \subseteq (d)$, $(g) \subseteq (d)$, and $d \in (f) + (g)$, which is equivalent to $(d) = (f) + (g)$, namely (3).

If (2) holds, since $d = uf + vg$, whenever $h \in K[X]$ divides f and g, then h divides d, and d is a gcd of f and g.

Assume that d is a gcd of f and g. Then, since d divides f and d divides g, we have $(f) \subseteq (d)$ and $(g) \subseteq (d)$, and thus $(f) + (g) \subseteq (d)$, and $(f) + (g)$ is nonempty since f and g are nonzero. By Proposition 30.10, there exists a monic polynomial $d_1 \in K[X]$ such that $(d_1) = (f) + (g)$. Then, d_1 divides both f and g, and since d is a gcd of f and g, then d_1 divides d, which shows that $(d) \subseteq (d_1) = (f) + (g)$. Consequently, $(f) + (g) = (d)$, and (3) holds.

Since $(d) = (f) + (g)$ and f and g are nonzero, the last part of the proposition is obvious. □

As a consequence of Proposition 30.11, two nonzero polynomials $f, g \in K[X]$ are relatively prime iff there exist $u, v \in K[X]$ such that

$$uf + vg = 1.$$

The identity

$$d = uf + vg$$

of part (2) of Proposition 30.11 is often called the *Bezout identity*.

We derive more useful consequences of Proposition 30.11.

Proposition 30.12. *Let K be a field and let $f, g \in K[X]$ be any two nonzero polynomials. For every gcd $d \in K[X]$ of f and g, the following properties hold:*

(1) For every nonzero polynomial $q \in K[X]$, the polynomial dq is a gcd of fq and gq.

(2) For every nonzero polynomial $q \in K[X]$, if q divides f and g, then d/q is a gcd of f/q and g/q.

Proof. (1) By Proposition 30.11 (2), d divides f and g, and there exist $u, v \in K[X]$, such that

$$d = uf + vg.$$

Then, dq divides fq and gq, and

$$dq = ufq + vgq.$$

By Proposition 30.11 (2), dq is a gcd of fq and gq. The proof of (2) is similar. □

The following proposition is used often.

Proposition 30.13. *(Euclid's proposition) Let K be a field and let $f, g, h \in K[X]$ be any nonzero polynomials. If f divides gh and f is relatively prime to g, then f divides h.*

Proof. From Proposition 30.11, f and g are relatively prime iff there exist some polynomials $u, v \in K[X]$ such that

$$uf + vg = 1.$$

Then, we have

$$ufh + vgh = h,$$

and since f divides gh, it divides both ufh and vgh, and so, f divides h. □

Proposition 30.14. *Let K be a field and let $f, g_1, \ldots, g_m \in K[X]$ be some nonzero polynomials. If f and g_i are relatively prime for all i, $1 \leq i \leq m$, then f and $g_1 \cdots g_m$ are relatively prime.*

Proof. We proceed by induction on m. The case $m = 1$ is trivial. Let $h = g_2 \cdots g_m$. By the induction hypothesis, f and h are relatively prime. Let d be a gcd of f and $g_1 h$. We claim that d is relatively prime to g_1. Otherwise, d and g_1 would have some nonconstant gcd d_1 which would divide both f and g_1, contradicting the fact that f and g_1 are relatively prime. Now, by Proposition 30.13, since d divides $g_1 h$ and d and g_1 are relatively prime, d divides $h = g_2 \cdots g_m$. But then, d is a divisor of f and h, and since f and h are relatively prime, d must be a constant, and f and $g_1 \cdots g_m$ are relatively prime. □

Definition 30.7 is generalized to any finite number of polynomials as follows.

Definition 30.8. Given any nonzero polynomials $f_1, \ldots, f_n \in K[X]$, where $n \geq 2$, a polynomial $d \in K[X]$ is a *greatest common divisor of* $f_1, \ldots, f_n$ (for short, a *gcd of* $f_1, \ldots, f_n$) if d divides each f_i and whenever $h \in K[X]$ divides each f_i, then h divides d. We say that $f_1, \ldots, f_n$ are *relatively prime* if 1 is a gcd of $f_1, \ldots, f_n$.

It is easily shown that Proposition 30.11 can be generalized to any finite number of polynomials, and similarly for its relevant corollaries. The details are left as an exercise.

Proposition 30.15. *Let K be a field and let $f_1, \ldots, f_n \in K[X]$ be any $n \geq 2$ nonzero polynomials. For every polynomial $d \in K[X]$, the following properties are equivalent:*

(1) The polynomial d is a gcd of $f_1, \ldots, f_n$.

(2) The polynomial d divides each f_i and there exist $u_1, \ldots, u_n \in K[X]$ such that

$$d = u_1 f_1 + \cdots + u_n f_n.$$

(3) The ideals (f_i), and (d) satisfy the equation

$$(d) = (f_1) + \cdots + (f_n).$$

In addition, $d \neq 0$, and d is unique up to multiplication by a nonzero scalar in K.

As a consequence of Proposition 30.15, some polynomials $f_1, \dots, f_n \in K[X]$ are relatively prime iff there exist $u_1, \dots, u_n \in K[X]$ such that

$$u_1 f_1 + \cdots + u_n f_n = 1.$$

The identity

$$u_1 f_1 + \cdots + u_n f_n = 1$$

of part (2) of Proposition 30.15 is also called the *Bezout identity*.

We now consider the factorization of polynomials of a single variable into irreducible factors.

30.5 Factorization and Irreducible Factors in $K[X]$

Definition 30.9. Given a field K, a polynomial $p \in K[X]$ is *irreducible or indecomposable or prime* if $\deg(p) \geq 1$ and if p is not divisible by any polynomial $q \in K[X]$ such that $1 \leq \deg(q) < \deg(p)$. Equivalently, p is irreducible if $\deg(p) \geq 1$ and if $p = q_1 q_2$, then either $q_1 \in K$ or $q_2 \in K$ (and of course, $q_1 \neq 0$, $q_2 \neq 0$).

Example 30.2. Every polynomial $aX + b$ of degree 1 is irreducible. Over the field $\mathbb{R}$, the polynomial $X^2 + 1$ is irreducible (why?), but $X^3 + 1$ is not irreducible, since

$$X^3 + 1 = (X + 1)(X^2 - X + 1).$$

The polynomial $X^2 - X + 1$ is irreducible over $\mathbb{R}$ (why?). It would seem that $X^4 + 1$ is irreducible over $\mathbb{R}$, but in fact,

$$X^4 + 1 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1).$$

However, in view of the above factorization, $X^4 + 1$ is irreducible over $\mathbb{Q}$.

It can be shown that the irreducible polynomials over $\mathbb{R}$ are the polynomials of degree 1, or the polynomials of degree 2 of the form $aX^2 + bX + c$, for which $b^2 - 4ac < 0$ (i.e., those having no real roots). This is not easy to prove! Over the complex numbers $\mathbb{C}$, the only irreducible polynomials are those of degree 1. This is a version of a fact often referred to as the "Fundamental theorem of Algebra", or, as the French sometimes say, as "d'Alembert's theorem"!

We already observed that for any two nonzero polynomials $f, g \in K[X]$, f divides g iff $(g) \subseteq (f)$. In view of the definition of a maximal ideal given in Definition 30.4, we now prove that a polynomial $p \in K[X]$ is irreducible iff (p) is a maximal ideal in $K[X]$.

Proposition 30.16. *A polynomial $p \in K[X]$ is irreducible iff (p) is a maximal ideal in $K[X]$.*

Proof. Since $K[X]$ is an integral domain, for all nonzero polynomials $p, q \in K[X]$, $\deg(pq) = \deg(p) + \deg(q)$, and thus, $(p) \neq K[X]$ iff $\deg(p) \geq 1$. Assume that $p \in K[X]$ is irreducible. Since every ideal in $K[X]$ is a principal ideal, every ideal in $K[X]$ is of the form (q), for some $q \in K[X]$. If $(p) \subseteq (q)$, with $\deg(q) \geq 1$, then q divides p, and since $p \in K[X]$ is irreducible, this implies that $p = \lambda q$ for some $\lambda \neq 0$ in K, and so, $(p) = (q)$. Thus, (p) is a maximal ideal. Conversely, assume that (p) is a maximal ideal. Then, as we showed above, $\deg(p) \geq 1$, and if q divides p, with $\deg(q) \geq 1$, then $(p) \subseteq (q)$, and since (p) is a maximal ideal, this implies that $(p) = (q)$, which means that $p = \lambda q$ for some $\lambda \neq 0$ in K, and so, p is irreducible. □

Let $p \in K[X]$ be irreducible. Then, for every nonzero polynomial $g \in K[X]$, either p and g are relatively prime, or p divides g. Indeed, if d is any gcd of p and g, if d is a constant, then p and g are relatively prime, and if not, because p is irreducible, we have $d = \lambda p$ for some $\lambda \neq 0$ in K, and thus, p divides g. As a consequence, if $p, q \in K[X]$ are both irreducible, then either p and q are relatively prime, or $p = \lambda q$ for some $\lambda \neq 0$ in K. In particular, if $p, q \in K[X]$ are both irreducible monic polynomials and $p \neq q$, then p and q are relatively prime.

We now prove the (unique) factorization of polynomials into irreducible factors.

Theorem 30.17. *Given any field K, for every nonzero polynomial*

$$f = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_0$$

of degree $d = \deg(f) \geq 1$ in $K[X]$, there exists a unique set $\{\langle p_1, k_1\rangle, \ldots, \langle p_m, k_m\rangle\}$ such that

$$f = a_d p_1^{k_1} \cdots p_m^{k_m},$$

where the $p_i \in K[X]$ are distinct irreducible monic polynomials, the k_i are (not necessarily distinct) integers, and $m \geq 1$, $k_i \geq 1$.

Proof. First, we prove the existence of such a factorization by induction on $d = \deg(f)$. Clearly, it is enough to prove the result for monic polynomials f of degree $d = \deg(f) \geq 1$. If $d = 1$, then $f = X + a_0$, which is an irreducible monic polynomial.

Assume $d \geq 2$, and assume the induction hypothesis for all monic polynomials of degree $< d$. Consider the set S of all monic polynomials g such that $\deg(g) \geq 1$ and g divides f. Since $f \in S$, the set S is nonempty, and thus, S contains some monic polynomial p_1 of minimal degree. Since $\deg(p_1) \geq 1$, the monic polynomial p_1 must be irreducible. Otherwise we would have $p_1 = g_1 g_2$, for some monic polynomials g_1, g_2 such that $\deg(p_1) > \deg(g_1) \geq 1$ and $\deg(p_1) > \deg(g_2) \geq 1$, and since p_1 divide f, then g_1 would divide f, contradicting the minimality of the degree of p_1. Thus, we have $f = p_1 q$, for some irreducible monic polynomial p_1, with q also monic. Since $\deg(p_1) \geq 1$, we have $\deg(q) < \deg(f)$, and we can apply the induction hypothesis to q. Thus, we obtain a factorization of the desired form.

We now prove uniqueness. Assume that

$$f = a_d p_1^{k_1} \cdots p_m^{k_m},$$

and

$$f = a_d q_1^{h_1} \cdots q_n^{h_n}.$$

Thus, we have

$$a_d p_1^{k_1} \cdots p_m^{k_m} = a_d q_1^{h_1} \cdots q_n^{h_n}.$$

We prove that $m = n$, $p_i = q_i$ and $h_i = k_i$, for all i, with $1 \leq i \leq n$.

The proof proceeds by induction on $h_1 + \cdots + h_n$.

If $h_1 + \cdots + h_n = 1$, then $n = 1$ and $h_1 = 1$. Then, since $K[X]$ is an integral domain, we have

$$p_1^{k_1} \cdots p_m^{k_m} = q_1,$$

and since q_1 and the p_i are irreducible monic, we must have $m = 1$ and $p_1 = q_1$.

If $h_1 + \cdots + h_n \geq 2$, since $K[X]$ is an integral domain and since $h_1 \geq 1$, we have

$$p_1^{k_1} \cdots p_m^{k_m} = q_1 q,$$

with

$$q = q_1^{h_1 - 1} \cdots q_n^{h_n},$$

where $(h_1 - 1) + \cdots + h_n \geq 1$ (and $q_1^{h_1 - 1} = 1$ if $h_1 = 1$). Now, if q_1 is not equal to any of the p_i, by a previous remark, q_1 and p_i are relatively prime, and by Proposition 30.14, q_1 and $p_1^{k_1} \cdots p_m^{k_m}$ are relatively prime. But this contradicts the fact that q_1 divides $p_1^{k_1} \cdots p_m^{k_m}$. Thus, q_1 is equal to one of the p_i. Without loss of generality, we can assume that $q_1 = p_1$. Then, since $K[X]$ is an integral domain, we have

$$p_1^{k_1 - 1} \cdots p_m^{k_m} = q_1^{h_1 - 1} \cdots q_n^{h_n},$$

where $p_1^{k_1 - 1} = 1$ if $k_1 = 1$, and $q_1^{h_1 - 1} = 1$ if $h_1 = 1$. Now, $(h_1 - 1) + \cdots + h_n < h_1 + \cdots + h_n$, and we can apply the induction hypothesis to conclude that $m = n$, $p_i = q_i$ and $h_i = k_i$, with $1 \leq i \leq n$. □

The above considerations about unique factorization into irreducible factors can be extended almost without changes to more general rings known as *Euclidean domains*. In such rings, some abstract version of the division theorem is assumed to hold.

Definition 30.10. A *Euclidean domain (or Euclidean ring)* is an integral domain A such that there exists a function $\varphi\colon A \to \mathbb{N}$ with the following property: For all $a, b \in A$ with $b \neq 0$, there are some $q, r \in A$ such that

$$a = bq + r \quad \text{and} \quad \varphi(r) < \varphi(b).$$

Note that the pair (q, r) is not necessarily unique.

Actually, unique factorization holds in principal ideal domains (PID's), see Theorem 32.12. As shown below, every Euclidean domain is a PID, and thus, unique factorization holds for Euclidean domains.

Proposition 30.18. *Every Euclidean domain A is a PID.*

Proof. Let $\mathfrak{I}$ be a nonnull ideal in A. Then, the set

$$\{\varphi(a) \mid a \in \mathfrak{I}\}$$

is nonempty, and thus, has a smallest element m. Let b be any (nonnull) element of $\mathfrak{I}$ such that $m = \varphi(b)$. We claim that $\mathfrak{I} = (b)$. Given any $a \in \mathfrak{I}$, we can write

$$a = bq + r$$

for some $q, r \in A$, with $\varphi(r) < \varphi(b)$. Since $b \in \mathfrak{I}$ and $\mathfrak{I}$ is an ideal, we also have $bq \in \mathfrak{I}$, and since $a, bq \in \mathfrak{I}$ and $\mathfrak{I}$ is an ideal, then $r \in \mathfrak{I}$ with $\varphi(r) < \varphi(b) = m$, contradicting the minimality of m. Thus, $r = 0$ and $a \in (b)$. But then,

$$\mathfrak{I} \subseteq (b),$$

and since $b \in \mathfrak{I}$, we get

$$\mathfrak{I} = (b),$$

and A is a PID. □

As a corollary of Proposition 30.18, the ring $\mathbb{Z}$ is a Euclidean domain (using the function $\varphi(a) = |a|$) and thus, a PID. If K is a field, the function φ on $K[X]$ defined such that

$$\varphi(f) = \begin{cases} 0 & \text{if } f = 0, \\ \deg(f) + 1 & \text{if } f \neq 0, \end{cases}$$

shows that $K[X]$ is a Euclidean domain.

Example 30.3. A more interesting example of a Euclidean domain is the ring $\mathbb{Z}[i]$ of *Gaussian integers*, i.e., the subring of $\mathbb{C}$ consisting of all complex numbers of the form $a + ib$, where $a, b \in \mathbb{Z}$. Using the function φ defined such that

$$\varphi(a + ib) = a^2 + b^2,$$

we leave it as an interesting exercise to prove that $\mathbb{Z}[i]$ is a Euclidean domain.

Not every PID is a Euclidean ring.

Remark: Given any integer $d \in \mathbb{Z}$ such that $d \neq 0, 1$ and d does not have any square factor greater than one, the *quadratic field* $\mathbb{Q}(\sqrt{d})$ is the field consisting of all complex numbers of the form $a + ib\sqrt{-d}$ if $d < 0$, and of all the real numbers of the form $a + b\sqrt{d}$ if $d > 0$, with $a, b \in \mathbb{Q}$. The subring of $\mathbb{Q}(\sqrt{d})$ consisting of all elements as above for which $a, b \in \mathbb{Z}$ is denoted by $\mathbb{Z}[\sqrt{d}]$. We define the *ring of integers* of the field $\mathbb{Q}(\sqrt{d})$ as the subring of $\mathbb{Q}(\sqrt{d})$ consisting of the following elements:

(1) If $d \equiv 2 \pmod 4$ or $d \equiv 3 \pmod 4$, then all elements of the form $a + ib\sqrt{-d}$ (if $d < 0$) or all elements of the form $a + b\sqrt{d}$ (if $d > 0$), with $a, b \in \mathbb{Z}$;

(2) If $d \equiv 1 \pmod 4$, then all elements of the form $(a + ib\sqrt{-d})/2$ (if $d < 0$) or all elements of the form $(a + b\sqrt{d})/2$ (if $d > 0$), with $a, b \in \mathbb{Z}$ and with a, b either both even or both odd.

Observe that when $d \equiv 2 \pmod 4$ or $d \equiv 3 \pmod 4$, the ring of integers of $\mathbb{Q}(\sqrt{d})$ is equal to $\mathbb{Z}[\sqrt{d}]$.

It can be shown that the rings of integers of the fields $\mathbb{Q}(\sqrt{-d})$ where $d = 19, 43, 67, 163$ are PID's, but not Euclidean rings. The proof is hard and long. First, it can be shown that these rings are UFD's (refer to Definition 32.2), see Stark [162] (Chapter 8, Theorems 8.21 and 8.22). Then, we use the fact that the ring of integers of the field $\mathbb{Q}(\sqrt{d})$ (with $d \neq 0, 1$ any square-free integers) is a certain kind of integral domain called a Dedekind ring; see Atiyah-MacDonald [8] (Chapter 9, Theorem 9.5) or Samuel [141] (Chapter III, Section 3.4). Finally, we use the fact that if a Dedekind ring is a UFD then it is a PID, which follows from Proposition 32.13.

Actually, the rings of integers of $\mathbb{Q}(\sqrt{d})$ that are Euclidean domains are completely determined but the proof is quite difficult. It turns out that there are twenty one such rings corresponding to the integers: $-11, -7, -3, -2, -1,\ 2, 3, 5, 6, 7, 11,\ 13, 17, 19, 21,\ 29, 33, 37, 41, 57$ and 73, see Stark [162] (Chapter 8). For more on quadratic fields and their rings of integers, see Stark [162] (Chapter 8) or Niven, Zuckerman and Montgomery [130] (Chapter 9).

It is possible to characterize a larger class of rings (in terms of ideals), *factorial rings (or unique factorization domains)*, for which unique factorization holds (see Section 32.1). We now consider zeros (or roots) of polynomials.

30.6 Roots of Polynomials

We go back to the general case of an arbitrary ring for a little while.

Definition 30.11. Given a ring A and any polynomial $f \in A[X]$, we say that some $\alpha \in A$ is *a zero of f, or a root of f*, if $f(\alpha) = 0$. Similarly, given a polynomial $f \in A[X_1, \ldots, X_n]$, we say that $(\alpha_1, \ldots, \alpha_n) \in A^n$ is a *a zero of f, or a root of f*, if $f(\alpha_1, \ldots, \alpha_n) = 0$.

When $f \in A[X]$ is the null polynomial, every $\alpha \in A$ is trivially a zero of f. This case being trivial, we usually assume that we are considering zeros of nonnull polynomials.

Example 30.4. Considering the polynomial $f(X) = X^2 - 1$, both $+1$ and -1 are zeros of $f(X)$. Over the field of reals, the polynomial $g(X) = X^2 + 1$ has no zeros. Over the field $\mathbb{C}$ of complex numbers, $g(X) = X^2 + 1$ has two roots i and $-i$, the square roots of -1, which are "imaginary numbers."

We have the following basic proposition showing the relationship between polynomial division and roots.

Proposition 30.19. *Let $f \in A[X]$ be any polynomial and $\alpha \in A$ any element of A. If the result of dividing f by $X - \alpha$ is $f = (X - \alpha)q + r$, then $r = 0$ iff $f(\alpha) = 0$, i.e., α is a root of f iff $r = 0$.*

Proof. We have $f = (X - \alpha)q + r$, with $\deg(r) < 1 = \deg(X - \alpha)$. Thus, r is a constant in K, and since $f(\alpha) = (\alpha - \alpha)q(\alpha) + r$, we get $f(\alpha) = r$, and the proposition is trivial. □

We now consider the issue of multiplicity of a root.

Proposition 30.20. *Let $f \in A[X]$ be any nonnull polynomial and $h \geq 0$ any integer. The following conditions are equivalent.*

(1) f is divisible by $(X - \alpha)^h$ but not by $(X - \alpha)^{h+1}$.

(2) There is some $g \in A[X]$ such that $f = (X - \alpha)^h g$ and $g(\alpha) \neq 0$.

Proof. Assume (1). Then, we have $f = (X - \alpha)^h g$ for some $g \in A[X]$. If we had $g(\alpha) = 0$, by Proposition 30.19, g would be divisible by $(X - \alpha)$, and then f would be divisible by $(X - \alpha)^{h+1}$, contradicting (1).

Assume (2), that is, $f = (X - \alpha)^h g$ and $g(\alpha) \neq 0$. If f is divisible by $(X - \alpha)^{h+1}$, then we have $f = (X - \alpha)^{h+1} g_1$, for some $g_1 \in A[X]$. Then, we have

$$(X - \alpha)^h g = (X - \alpha)^{h+1} g_1,$$

and thus

$$(X - \alpha)^h (g - (X - \alpha) g_1) = 0,$$

and since the leading coefficient of $(X - \alpha)^h$ is 1 (show this by induction), by Proposition 30.1, $(X - \alpha)^h$ is not a zero divisor, and we get $g - (X - \alpha)g_1 = 0$, i.e., $g = (X - \alpha)g_1$, and so $g(\alpha) = 0$, contrary to the hypothesis. □

As a consequence of Proposition 30.20, for every nonnull polynomial $f \in A[X]$ and every $\alpha \in A$, there is a unique integer $h \geq 0$ such that f is divisible by $(X - \alpha)^h$ but not by $(X - \alpha)^{h+1}$. Indeed, since f is divisible by $(X - \alpha)^h$, we have $h \leq \deg(f)$. When $h = 0$, α is not a root of f, i.e., $f(\alpha) \neq 0$. The interesting case is when α is a root of f.

Definition 30.12. Given a ring A and any nonnull polynomial $f \in A[X]$, given any $\alpha \in A$, the unique $h \geq 0$ such that f is divisible by $(X - \alpha)^h$ but not by $(X - \alpha)^{h+1}$ is called the *order, or multiplicity, of* α. We have $h = 0$ iff α is not a root of f, and when α is a root of f, if $h = 1$, we call α a *simple root*, if $h = 2$, a *double root*, and generally, a root of multiplicity $h \geq 2$ is called a *multiple root*.

Observe that Proposition 30.20 (2) implies that if $A \subseteq B$, where A and B are rings, for every nonnull polynomial $f \in A[X]$, if $\alpha \in A$ is a root of f, then the multiplicity of α with respect to $f \in A[X]$ and the multiplicity of α with respect to f considered as a polynomial in $B[X]$, is the same.

We now show that if the ring A is an integral domain, the number of roots of a nonzero polynomial is at most its degree.

Proposition 30.21. *Let $f, g \in A[X]$ be nonnull polynomials, let $\alpha \in A$, and let $h \geq 0$ and $k \geq 0$ be the multiplicities of α with respect to f and g. The following properties hold.*

(1) If l is the multiplicity of α with respect to $(f + g)$, then $l \geq \min(h, k)$. If $h \neq k$, then $l = \min(h, k)$.

(2) If m is the multiplicity of α with respect to fg, then $m \geq h + k$. If A is an integral domain, then $m = h + k$.

Proof. (1) We have $f(X) = (X - \alpha)^h f_1(X)$, $g(X) = (X - \alpha)^k g_1(X)$, with $f_1(\alpha) \neq 0$ and $g_1(\alpha) \neq 0$. Clearly, $l \geq \min(h, k)$. If $h \neq k$, assume $h < k$. Then, we have

$$f(X) + g(X) = (X - \alpha)^h f_1(X) + (X - \alpha)^k g_1(X) = (X - \alpha)^h (f_1(X) + (X - \alpha)^{k-h} g_1(X)),$$

and since $(f_1(X) + (X - \alpha)^{k-h} g_1(X))(\alpha) = f_1(\alpha) \neq 0$, we have $l = h = \min(h, k)$.

(2) We have

$$f(X)g(X) = (X - \alpha)^{h+k} f_1(X) g_1(X),$$

with $f_1(\alpha) \neq 0$ and $g_1(\alpha) \neq 0$. Clearly, $m \geq h + k$. If A is an integral domain, then $f_1(\alpha) g_1(\alpha) \neq 0$, and so $m = h + k$. □

Proposition 30.22. *Let A be an integral domain. Let f be any nonnull polynomial $f \in A[X]$ and let $\alpha_1, \ldots, \alpha_m \in A$ be $m \geq 1$ distinct roots of f of respective multiplicities $k_1, \ldots, k_m$. Then, we have*

$$f(X) = (X - \alpha_1)^{k_1} \cdots (X - \alpha_m)^{k_m} g(X),$$

where $g \in A[X]$ and $g(\alpha_i) \neq 0$ for all i, $1 \leq i \leq m$.

Proof. We proceed by induction on m. The case $m = 1$ is obvious in view of Definition 30.12 (which itself, is justified by Proposition 30.20). If $m \geq 2$, by the induction hypothesis, we have

$$f(X) = (X - \alpha_1)^{k_1} \cdots (X - \alpha_{m-1})^{k_{m-1}} g_1(X),$$

where $g_1 \in A[X]$ and $g_1(\alpha_i) \neq 0$, for $1 \leq i \leq m-1$. Since A is an integral domain and $\alpha_i \neq \alpha_j$ for $i \neq j$, since α_m is a root of f, we have

$$0 = (\alpha_m - \alpha_1)^{k_1} \cdots (\alpha_m - \alpha_{m-1})^{k_{m-1}} g_1(\alpha_m),$$

which implies that $g_1(\alpha_m) = 0$. Now, by Proposition 30.21 (2), since α_m is not a root of the polynomial $(X - \alpha_1)^{k_1} \cdots (X - \alpha_{m-1})^{k_{m-1}}$ and since A is an integral domain, α_m must be a root of multiplicity k_m of g_1, which means that

$$g_1(X) = (X - \alpha_m)^{k_m} g(X),$$

with $g(\alpha_m) \neq 0$. Since $g_1(\alpha_i) \neq 0$ for $1 \leq i \leq m-1$ and A is an integral domain, we must also have $g(\alpha_i) \neq 0$, for $1 \leq i \leq m-1$. Thus, we have

$$f(X) = (X - \alpha_1)^{k_1} \cdots (X - \alpha_m)^{k_m} g(X),$$

where $g \in A[X]$, and $g(\alpha_i) \neq 0$ for $1 \leq i \leq m$. □

As a consequence of Proposition 30.22, we get the following important result.

Theorem 30.23. *Let A be an integral domain. For every nonnull polynomial $f \in A[X]$, if the degree of f is $n = \deg(f)$ and $k_1, \ldots, k_m$ are the multiplicities of all the distinct roots of f (where $m \geq 0$), then $k_1 + \cdots + k_m \leq n$.*

Proof. Immediate from Proposition 30.22. □

Since fields are integral domains, Theorem 30.23 holds for nonnull polynomials over fields and in particular, for $\mathbb{R}$ and $\mathbb{C}$. An important consequence of Theorem 30.23 is the following.

Proposition 30.24. *Let A be an integral domain. For any two polynomials $f, g \in A[X]$, if $\deg(f) \leq n$, $\deg(g) \leq n$, and if there are $n+1$ distinct elements $\alpha_1, \alpha_2, \ldots, \alpha_{n+1} \in A$ (with $\alpha_i \neq \alpha_j$ for $i \neq j$) such that $f(\alpha_i) = g(\alpha_i)$ for all i, $1 \leq i \leq n+1$, then $f = g$.*

Proof. Assume $f \neq g$, then, $(f - g)$ is nonnull, and since $f(\alpha_i) = g(\alpha_i)$ for all i, $1 \leq i \leq n+1$, the polynomial $(f - g)$ has $n+1$ distinct roots. Thus, $(f - g)$ has $n+1$ distinct roots and is of degree at most n, which contradicts Theorem 30.23. □

Proposition 30.24 is often used to show that polynomials coincide. We will use it to show some interpolation formulae due to Lagrange and Hermite. But first, we characterize the multiplicity of a root of a polynomial. For this, we need the notion of derivative familiar in analysis. Actually, we can simply define this notion algebraically.

First, we need to rule out some undesirable behaviors. Given a field K, as we saw in Example 2.8, we can define a homomorphism $\chi\colon \mathbb{Z} \to K$ given by

$$\chi(n) = n \cdot 1,$$

where 1 is the multiplicative identity of K. Recall that we define $n \cdot a$ by

$$n \cdot a = \underbrace{a + \cdots + a}_{n}$$

if $n \geq 0$ (with $0 \cdot a = 0$) and

$$n \cdot a = -(-n) \cdot a$$

if $n < 0$. We say that the field K is of *characteristic zero* if the homomorphism χ is injective. Then, for any $a \in K$ with $a \neq 0$, we have $n \cdot a \neq 0$ for all $n \neq 0$

The fields $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are of characteristic zero. In fact, it is easy to see that every field of characteristic zero contains a subfield isomorphic to $\mathbb{Q}$. Thus, finite fields can't be of characteristic zero.

Remark: If a field is not of characteristic zero, it is not hard to show that its characteristic, that is, the smallest $n \geq 2$ such that $n \cdot 1 = 0$, is a prime number p. The characteristic p of K is the generator of the principal ideal $p\mathbb{Z}$, the kernel of the homomorphism $\chi \colon \mathbb{Z} \to K$. Thus, every finite field is of characteristic some prime p. Infinite fields of nonzero characteristic also exist.

Definition 30.13. Let A be a ring. The *derivative f', or $\mathrm{D}f$, or $\mathrm{D}^1 f$, of a polynomial* $f \in A[X]$ is defined inductively as follows:

$$\begin{aligned}
f' &= 0, \quad \text{if } f = 0, \text{ the null polynomial,}\\
f' &= 0, \quad \text{if } f = a,\ a \neq 0,\ a \in A,\\
f' &= na_n X^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + 2a_2 X + a_1,\\
&\qquad\quad \text{if } f = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0, \ \text{ with } n = \deg(f) \geq 1.
\end{aligned}$$

If $A = K$ is a field of characteristic zero, if $\deg(f) \geq 1$, the leading coefficient na_n of f' is nonzero, and thus, f' is not the null polynomial. Thus, if $A = K$ is a field of characteristic zero, when $n = \deg(f) \geq 1$, we have $\deg(f') = n - 1$.

For rings or for fields of characteristic $p \geq 2$, we could have $f' = 0$, for a polynomial f of degree ≥ 1.

The following standard properties of derivatives are recalled without proof (prove them as an exercise).

Given any two polynomials, $f, g \in A[X]$, we have

$$\begin{aligned}
(f + g)' &= f' + g',\\
(fg)' &= f'g + fg'.
\end{aligned}$$

For example, if $f = (X - \alpha)^k g$ and $k \geq 1$, we have

$$f' = k(X - \alpha)^{k-1}g + (X - \alpha)^k g'.$$

We can now give a criterion for the existence of simple roots. The first proposition holds for any ring.

Proposition 30.25. *Let A be any ring. For every nonnull polynomial $f \in A[X]$, $\alpha \in A$ is a simple root of f iff α is a root of f and α is not a root of f'.*

Proof. Since $\alpha \in A$ is a root of f, we have $f = (X - \alpha)g$ for some $g \in A[X]$. Now, α is a simple root of f iff $g(\alpha) \neq 0$. However, we have $f' = g + (X - \alpha)g'$, and so $f'(\alpha) = g(\alpha)$. Thus, α is a simple root of f iff $f'(\alpha) \neq 0$. □

We can improve the previous proposition as follows.

Proposition 30.26. *Let A be any ring. For every nonnull polynomial $f \in A[X]$, let $\alpha \in A$ be a root of multiplicity $k \geq 1$ of f. Then, α is a root of multiplicity at least $k - 1$ of f'. If A is a field of characteristic zero, then α is a root of multiplicity $k - 1$ of f'.*

Proof. Since $\alpha \in A$ is a root of multiplicity k of f, we have $f = (X - \alpha)^k g$ for some $g \in A[X]$ and $g(\alpha) \neq 0$. Since

$$f' = k(X - \alpha)^{k-1} g + (X - \alpha)^k g' = (X - \alpha)^{k-1}(kg + (X - \alpha)g'),$$

it is clear that the multiplicity of α w.r.t. f' is at least $k-1$. Now, $(kg+(X-\alpha)g')(\alpha) = kg(\alpha)$, and if A is of characteristic zero, since $g(\alpha) \neq 0$, then $kg(\alpha) \neq 0$. Thus, α is a root of multiplicity $k - 1$ of f'. □

As a consequence, we obtain the following test for the existence of a root of multiplicity k for a polynomial f:

Given a field K of characteristic zero, for any nonnull polynomial $f \in K[X]$, any $\alpha \in K$ is a root of multiplicity $k \geq 1$ of f iff α is a root of $f, \mathrm{D}^1 f, \mathrm{D}^2 f, \ldots, \mathrm{D}^{k-1} f$, but not a root of $\mathrm{D}^k f$.

We can now return to polynomial functions and tie up some loose ends. Given a ring A, recall that every polynomial $f \in A[X_1, \ldots, X_n]$ induces a function $f_A \colon A^n \to A$ defined such that $f_A(\alpha_1, \ldots, \alpha_n) = f(\alpha_1, \ldots, \alpha_n)$, for every $(\alpha_1, \ldots, \alpha_n) \in A^n$. We now give a sufficient condition for the mapping $f \mapsto f_A$ to be injective.

Proposition 30.27. *Let A be an integral domain. For every polynomial $f \in A[X_1, \ldots, X_n]$, if $A_1, \ldots, A_n$ are n infinite subsets of A such that $f(\alpha_1, \ldots, \alpha_n) = 0$ for all $(\alpha_1, \ldots, \alpha_n) \in A_1 \times \cdots \times A_n$, then $f = 0$, i.e., f is the null polynomial. As a consequence, if A is an infinite integral domain, then the map $f \mapsto f_A$ is injective.*

Proof. We proceed by induction on n. Assume $n = 1$. If $f \in A[X_1]$ is nonnull, let $m = \deg(f)$ be its degree. Since A_1 is infinite and $f(\alpha_1) = 0$ for all $\alpha_1 \in A_1$, then f has an infinite number of roots. But since f is of degree m, this contradicts Theorem 30.23. Thus, $f = 0$.

If $n \geq 2$, we can view $f \in A[X_1, \ldots, X_n]$ as a polynomial

$$f = g_m X_n^m + g_{m-1} X_n^{m-1} + \cdots + g_0,$$

where the coefficients g_i are polynomials in $A[X_1, \ldots, X_{n-1}]$. Now, for every $(\alpha_1, \ldots, \alpha_{n-1}) \in A_1 \times \cdots \times A_{n-1}$, $f(\alpha_1, \ldots, \alpha_{n-1}, X_n)$ determines a polynomial $h(X_n) \in A[X_n]$, and since A_n is infinite and $h(\alpha_n) = f(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n) = 0$ for all $\alpha_n \in A_n$, by the induction hypothesis, we have $g_i(\alpha_1, \ldots, \alpha_{n-1}) = 0$. Now, since $A_1, \ldots, A_{n-1}$ are infinite, using the induction hypothesis again, we get $g_i = 0$, which shows that f is the null polynomial. The second part of the proposition follows immediately from the first, by letting $A_i = A$. □

When A is an infinite integral domain, in particular an infinite field, since the map $f \mapsto f_A$ is injective, we identify the polynomial f with the polynomial function f_A, and we write f_A simply as f.

The following proposition can be very useful to show polynomial identities.

Proposition 30.28. *Let A be an infinite integral domain and $f, g_1, \ldots, g_m \in A[X_1, \ldots, X_n]$ be polynomials. If the g_i are nonnull polynomials and if*

$$f(\alpha_1, \ldots, \alpha_n) = 0 \textit{ whenever } g_i(\alpha_1, \ldots, \alpha_n) \neq 0 \textit{ for all } i,\ 1 \leq i \leq m,$$

for every $(\alpha_1, \ldots, \alpha_n) \in A^n$, then

$$f = 0,$$

i.e., f is the null polynomial.

Proof. If f is not the null polynomial, since the g_i are nonnull and A is an integral domain, then the product $fg_1 \cdots g_m$ is nonnull. By Proposition 30.27, only the null polynomial maps to the zero function, and thus there must be some $(\alpha_1, \ldots, \alpha_n) \in A^n$, such that

$$f(\alpha_1, \ldots, \alpha_n)g_1(\alpha_1, \ldots, \alpha_n) \cdots g_m(\alpha_1, \ldots, \alpha_n) \neq 0,$$

but this contradicts the hypothesis. □

Proposition 30.28 is often called the *principle of extension of algebraic identities*. Another perhaps more illuminating way of stating this proposition is as follows: For any polynomial $g \in A[X_1, \ldots, X_n]$, let

$$V(g) = \{(\alpha_1, \ldots, \alpha_n) \in A^n \mid g(\alpha_1, \ldots, \alpha_n) = 0\},$$

the set of zeros of g. Note that $V(g_1) \cup \cdots \cup V(g_m) = V(g_1 \cdots g_m)$. Then, Proposition 30.28 can be stated as:

If $f(\alpha_1, \ldots, \alpha_n) = 0$ for every $(\alpha_1, \ldots, \alpha_n) \in A^n - V(g_1 \cdots g_m)$, then $f = 0$.

In other words, if the algebraic identity $f(\alpha_1, \ldots, \alpha_n) = 0$ holds on the complement of $V(g_1) \cup \cdots \cup V(g_m) = V(g_1 \cdots g_m)$, then $f(\alpha_1, \ldots, \alpha_n) = 0$ holds everywhere in A^n. With this second formulation, we understand better the terminology "principle of extension of algebraic identities."

Remark: Letting $U(g) = A - V(g)$, the identity $V(g_1) \cup \cdots \cup V(g_m) = V(g_1 \cdots g_m)$ translates to $U(g_1) \cap \cdots \cap U(g_m) = U(g_1 \cdots g_m)$. This suggests to define a topology on A whose basis of open sets consists of the sets $U(g)$. In this topology (called the Zariski topology), the sets of the form $V(g)$ are closed sets. Also, when $g_1, \ldots, g_m \in A[X_1, \ldots, X_n]$ and $n \geq 2$, understanding the structure of the closed sets of the form $V(g_1) \cap \cdots \cap V(g_m)$ is quite difficult, and it is the object of algebraic geometry (at least, its classical part).

When $f \in A[X_1, \ldots, X_n]$ and $n \geq 2$, one should not apply Proposition 30.27 abusively. For example, let

$$f(X, Y) = X^2 + Y^2 - 1,$$

considered as a polynomial in $\mathbb{R}[X, Y]$. Since $\mathbb{R}$ is an infinite field and since

$$f\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) = \frac{(1-t^2)^2}{(1+t^2)^2} + \frac{(2t)^2}{(1+t^2)^2} - 1 = 0,$$

for every $t \in \mathbb{R}$, it would be tempting to say that $f = 0$. But what's wrong with the above reasoning is that there are no two infinite subsets R_1, R_2 of $\mathbb{R}$ such that $f(\alpha_1, \alpha_2) = 0$ for all $(\alpha_1, \alpha_2) \in \mathbb{R}^2$. For every $\alpha_1 \in \mathbb{R}$, there are at most two $\alpha_2 \in \mathbb{R}$ such that $f(\alpha_1, \alpha_2) = 0$. What the example shows though, is that a nonnull polynomial $f \in A[X_1, \ldots, X_n]$ where $n \geq 2$ can have an infinite number of zeros. This is in contrast with nonnull polynomials in one variables over an infinite field (which have a number of roots bounded by their degree).

We now look at polynomial interpolation.

30.7 Polynomial Interpolation (Lagrange, Newton, Hermite)

Let K be a field. First, we consider the following interpolation problem: Given a sequence $(\alpha_1, \ldots, \alpha_{m+1})$ of pairwise distinct scalars in K and any sequence $(\beta_1, \ldots, \beta_{m+1})$ of scalars in K, where the β_j are not necessarily distinct, find a polynomial $P(X)$ of degree $\leq m$ such that

$$P(\alpha_1) = \beta_1, \ldots, P(\alpha_{m+1}) = \beta_{m+1}.$$

First, observe that if such a polynomial exists, then it is unique. Indeed, this is a consequence of Proposition 30.24. Thus, we just have to find any polynomial of degree $\leq m$. Consider the following so-called *Lagrange polynomials*:

$$L_i(X) = \frac{(X - \alpha_1) \cdots (X - \alpha_{i-1})(X - \alpha_{i+1}) \cdots (X - \alpha_{m+1})}{(\alpha_i - \alpha_1) \cdots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \cdots (\alpha_i - \alpha_{m+1})}.$$

Note that $L(\alpha_i) = 1$ and that $L(\alpha_j) = 0$, for all $j \neq i$. But then,

$$P(X) = \beta_1 L_1 + \cdots + \beta_{m+1} L_{m+1}$$

is the unique desired polynomial, since clearly, $P(\alpha_i) = \beta_i$. Such a polynomial is called a *Lagrange interpolant*. Also note that the polynomials $(L_1, \ldots, L_{m+1})$ form a basis of the vector space of all polynomials of degree $\leq m$. Indeed, if we had

$$\lambda_1 L_1(X) + \cdots + \lambda_{m+1} L_{m+1}(X) = 0,$$

setting X to α_i, we would get $\lambda_i = 0$. Thus, the L_i are linearly independent, and by the previous argument, they are a set of generators. We we call $(L_1, \ldots, L_{m+1})$ the *Lagrange basis* (of order $m + 1$).

It is known from numerical analysis that from a computational point of view, the Lagrange basis is not very good. Newton proposed another solution, the method of divided differences.

Consider the polynomial $P(X)$ of degree $\leq m$, called the *Newton interpolant*,

$$P(X) = \lambda_0 + \lambda_1(X - \alpha_1) + \lambda_2(X - \alpha_1)(X - \alpha_2) + \cdots + \lambda_m(X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_m).$$

Then, the λ_i can be determined by successively setting X to, $\alpha_1, \alpha_2, \ldots, \alpha_{m+1}$. More precisely, we define inductively the polynomials $Q(X)$ and $Q(\alpha_1, \ldots, \alpha_i, X)$, for $1 \leq i \leq m$, as follows:

$$\begin{aligned}
Q(X) &= P(X) \\
Q_1(\alpha_1, X) &= \frac{Q(X) - Q(\alpha_1)}{X - \alpha_1} \\
Q(\alpha_1, \alpha_2, X) &= \frac{Q(\alpha_1, X) - Q(\alpha_1, \alpha_2)}{X - \alpha_2} \\
&\cdots \\
Q(\alpha_1, \ldots, \alpha_i, X) &= \frac{Q(\alpha_1, \ldots, \alpha_{i-1}, X) - Q(\alpha_1, \ldots, \alpha_{i-1}, \alpha_i)}{X - \alpha_i}, \\
&\cdots \\
Q(\alpha_1, \ldots, \alpha_m, X) &= \frac{Q(\alpha_1, \ldots, \alpha_{m-1}, X) - Q(\alpha_1, \ldots, \alpha_{m-1}, \alpha_m)}{X - \alpha_m}.
\end{aligned}$$

By induction on i, $1 \leq i \leq m - 1$, it is easily verified that

$$\begin{aligned}
Q(X) &= P(X), \\
Q(\alpha_1, \ldots, \alpha_i, X) &= \lambda_i + \lambda_{i+1}(X - \alpha_{i+1}) + \cdots + \lambda_m(X - \alpha_{i+1})\cdots(X - \alpha_m), \\
Q(\alpha_1, \ldots, \alpha_m, X) &= \lambda_m.
\end{aligned}$$

From the above expressions, it is clear that

$$\begin{aligned}
\lambda_0 &= Q(\alpha_1), \\
\lambda_i &= Q(\alpha_1, \ldots, \alpha_i, \alpha_{i+1}), \\
\lambda_m &= Q(\alpha_1, \ldots, \alpha_m, \alpha_{m+1}).
\end{aligned}$$

The expression $Q(\alpha_1, \alpha_2, \ldots, \alpha_{i+1})$ is called the *i-th difference quotient*. Then, we can compute the λ_i in terms of $\beta_1 = P(\alpha_1), \ldots, \beta_{m+1} = P(\alpha_{m+1})$, using the inductive formulae for the $Q(\alpha_1, \ldots, \alpha_i, X)$ given above, initializing the $Q(\alpha_i)$ such that $Q(\alpha_i) = \beta_i$.

The above method is called the method of *divided differences* and it is due to Newton.

An astute observation may be used to optimize the computation. Observe that if $P_i(X)$ is the polynomial of degree $\leq i$ taking the values $\beta_1, \ldots, \beta_{i+1}$ at the points $\alpha_1, \ldots, \alpha_{i+1}$, then the coefficient of X^i in $P_i(X)$ is $Q(\alpha_1, \alpha_2, \ldots, \alpha_{i+1})$, which is the value of λ_i in the Newton interpolant

$$P_i(X) = \lambda_0 + \lambda_1(X - \alpha_1) + \lambda_2(X - \alpha_1)(X - \alpha_2) + \cdots + \lambda_i(X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_i).$$

As a consequence, $Q(\alpha_1, \alpha_2, \ldots, \alpha_{i+1})$ does not depend on the specific ordering of the α_j and there are better ways of computing it. For example, $Q(\alpha_1, \alpha_2, \ldots, \alpha_{i+1})$ can be computed using

$$Q(\alpha_1, \ldots, \alpha_{i+1}) = \frac{Q(\alpha_2, \ldots, \alpha_{i+1}) - Q(\alpha_1, \ldots, \alpha_i)}{\alpha_{i+1} - \alpha_1}.$$

Then, the computation can be arranged into a triangular array reminiscent of Pascal's triangle, as follows:

Initially, $Q(\alpha_j) = \beta_j$, $1 \leq j \leq m + 1$, and

$$\begin{array}{llll}
Q(\alpha_1) & & & \\
 & Q(\alpha_1, \alpha_2) & & \\
Q(\alpha_2) & & Q(\alpha_1, \alpha_2, \alpha_3) & \\
 & Q(\alpha_2, \alpha_3) & & \ldots \\
Q(\alpha_3) & & Q(\alpha_2, \alpha_3, \alpha_4) & \\
 & Q(\alpha_3, \alpha_4) & \ldots & \\
Q(\alpha_4) & \ldots & & \\
\ldots & & &
\end{array}$$

In this computation, each successive column is obtained by forming the difference quotients of the preceeding column according to the formula

$$Q(\alpha_k, \ldots, \alpha_{i+k}) = \frac{Q(\alpha_{k+1}, \ldots, \alpha_{i+k}) - Q(\alpha_k, \ldots, \alpha_{i+k-1})}{\alpha_{i+k} - \alpha_k}.$$

The λ_i are the elements of the descending diagonal.

Observe that if we performed the above computation starting with a polynomial $Q(X)$ of degree m, we could extend it by considering new given points α_{m+2}, α_{m+3}, etc. Then, from what we saw above, the $(m+1)$th column consists of λ_m in the expression of $Q(X)$ as a Newton interpolant and the $(m+2)$th column consists of zeros. Such divided differences are used in numerical analysis.

Newton's method can be used to compute the value $P(\alpha)$ at some α of the interpolant $P(X)$ taking the values $\beta_1, \ldots, \beta_{m+1}$ for the (distinct) arguments $\alpha_1, \ldots, \alpha_{m+1}$. We also mention that inductive methods for computing $P(\alpha)$ without first computing the coefficients of the Newton interpolant exist, for example, Aitken's method. For this method, the reader is referred to Farin [59].

It has been observed that Lagrange interpolants oscillate quite badly as their degree increases, and thus, this makes them undesirable as a stable method for interpolation. A standard example due to Runge, is the function

$$f(x) = \frac{1}{1+x^2},$$

in the interval $[-5, +5]$. Assuming a uniform distribution of points on the curve in the interval $[-5, +5]$, as the degree of the Lagrange interpolant increases, the interpolant shows wilder and wilder oscillations around the points $x = -5$ and $x = +5$. This phenomenon becomes quite noticeable beginning for degree 14, and gets worse and worse. For degree 22, things are quite bad! Equivalently, one may consider the function

$$f(x) = \frac{1}{1+25x^2},$$

in the interval $[-1, +1]$.

We now consider a more general interpolation problem which will lead to the Hermite polynomials.

We consider the following interpolation problem:

Given a sequence $(\alpha_1, \ldots, \alpha_{m+1})$ of pairwise distinct scalars in K, integers $n_1, \ldots, n_{m+1}$ where $n_j \geq 0$, and $m+1$ sequences $(\beta_j^0, \ldots, \beta_j^{n_j})$ of scalars in K, letting

$$n = n_1 + \cdots + n_{m+1} + m,$$

find a polynomial P of degree $\leq n$, such that

$$\begin{array}{rcr}
P(\alpha_1) = \beta_1^0, & \ldots & P(\alpha_{m+1}) = \beta_{m+1}^0, \\
\mathrm{D}^1 P(\alpha_1) = \beta_1^1, & \ldots & \mathrm{D}^1 P(\alpha_{m+1}) = \beta_{m+1}^1, \\
 & \ldots & \\
\mathrm{D}^i P(\alpha_1) = \beta_1^i, & \ldots & \mathrm{D}^i P(\alpha_{m+1}) = \beta_{m+1}^i, \\
 & \ldots & \\
\mathrm{D}^{n_1} P(\alpha_1) = \beta_1^{n_1}, & \ldots & \mathrm{D}^{n_{m+1}} P(\alpha_{m+1}) = \beta_{m+1}^{n_{m+1}}.
\end{array}$$

Note that the above equations constitute $n+1$ constraints, and thus, we can expect that there is a unique polynomial of degree $\leq n$ satisfying the above problem. This is indeed the case and such a polynomial is called a *Hermite polynomial*. We call the above problem the *Hermite interpolation problem*.

Proposition 30.29. *The Hermite interpolation problem has a unique solution of degree $\leq n$, where $n = n_1 + \cdots + n_{m+1} + m$.*

Proof. First, we prove that the Hermite interpolation problem has at most one solution. Assume that P and Q are two distinct solutions of degree $\leq n$. Then, by Proposition 30.26 and the criterion following it, $P - Q$ has among its roots α_1 of multiplicity at least $n_1 + 1, \ldots$, α_{m+1} of multiplicity at least $n_{m+1} + 1$. However, by Theorem 30.23, we should have

$$n_1 + 1 + \cdots + n_{m+1} + 1 = n_1 + \cdots + n_{m+1} + m + 1 \leq n,$$

which is a contradiction, since $n = n_1 + \cdots + n_{m+1} + m$. Thus, $P = Q$. We are left with proving the existence of a Hermite interpolant. A quick way to do so is to use Proposition 7.12, which tells us that given a square matrix A over a field K, the following properties hold:

For every column vector B, there is a unique column vector X such that $AX = B$ iff the only solution to $AX = 0$ is the trivial vector $X = 0$ iff $D(A) \neq 0$.

If we let $P = y_0 + y_1 X + \cdots + y_n X^n$, the Hermite interpolation problem yields a linear system of equations in the unknowns $(y_0, \ldots, y_n)$ with some associated $(n+1) \times (n+1)$ matrix A. Now, the system $AY = 0$ has a solution iff P has among its roots α_1 of multiplicity at least $n_1 + 1, \ldots$, α_{m+1} of multiplicity at least $n_{m+1} + 1$. By the previous argument, since P has degree $\leq n$, we must have $P = 0$, that is, $Y = 0$. This concludes the proof. $\square$

Proposition 30.29 shows the existence of unique polynomials $H^i_j(X)$ of degree $\leq n$ such that $\mathrm{D}^i H^i_j(\alpha_j) = 1$ and $\mathrm{D}^k H^i_j(\alpha_l) = 0$, for $k \neq i$ or $l \neq j$, $1 \leq j, l \leq m + 1$, $0 \leq i, k \leq n_j$. The polynomials H^i_j are called *Hermite basis polynomials*.

One problem with Proposition 30.29 is that it does not give an explicit way of computing the Hermite basis polynomials. We first show that this can be done explicitly in the special cases $n_1 = \ldots = n_{m+1} = 1$, and $n_1 = \ldots = n_{m+1} = 2$, and then suggest a method using a generalized Newton interpolant.

Assume that $n_1 = \ldots = n_{m+1} = 1$. We try $H^0_j = (a(X - \alpha_j) + b)L^2_j$, and $H^1_j = (c(X - \alpha_j) + d)L^2_j$, where L_j is the Lagrange interpolant determined earlier. Since

$$\mathrm{D}H^0_j = aL^2_j + 2(a(X - \alpha_j) + b)L_j \mathrm{D}L_j,$$

requiring that $H^0_j(\alpha_j) = 1$, $H^0_j(\alpha_k) = 0$, $\mathrm{D}H^0_j(\alpha_j) = 0$, and $\mathrm{D}H^0_j(\alpha_k) = 0$, for $k \neq j$, implies $b = 1$ and $a = -2\mathrm{D}L_j(\alpha_j)$. Similarly, from the requirements $H^1_j(\alpha_j) = 0$, $H^1_j(\alpha_k) = 0$, $\mathrm{D}H^1_j(\alpha_j) = 1$, and $\mathrm{D}H^1_j(\alpha_k) = 0$, $k \neq j$, we get $c = 1$ and $d = 0$.

Thus, we have the Hermite polynomials

$$H^0_j = (1 - 2\mathrm{D}L_j(\alpha_j)(X - \alpha_j))L^2_j, \qquad H^1_j = (X - \alpha_j)L^2_j.$$

In the special case where $m = 1$, $\alpha_1 = 0$, and $\alpha_2 = 1$, we leave as an exercise to show that the Hermite polynomials are

$$\begin{aligned}H_0^0 &= 2X^3 - 3X^2 + 1,\\ H_1^0 &= -2X^3 + 3X^2,\\ H_0^1 &= X^3 - 2X^2 + X,\\ H_1^1 &= X^3 - X^2.\end{aligned}$$

As a consequence, the polynomial P of degree 3 such that $P(0) = x_0$, $P(1) = x_1$, $P'(0) = m_0$, and $P'(1) = m_1$, can be written as

$$P(X) = x_0(2X^3 - 3X^2 + 1) + m_0(X^3 - 2X^2 + X) + m_1(X^3 - X^2) + x_1(-2X^3 + 3X^2).$$

If we want the polynomial P of degree 3 such that $P(a) = x_0$, $P(b) = x_1$, $P'(a) = m_0$, and $P'(b) = m_1$, where $b \neq a$, then we have

$$P(X) = x_0(2t^3 - 3t^2 + 1) + (b-a)m_0(t^3 - 2t^2 + t) + (b-a)m_1(t^3 - t^2) + x_1(-2t^3 + 3t^2),$$

where

$$t = \frac{X-a}{b-a}.$$

Observe the presence of the extra factor $(b - a)$ in front of m_0 and m_1, the formula would be false otherwise!

We now consider the case where $n_1 = \ldots = n_{m+1} = 2$. Let us try

$$H_j^i(X) = (a^i(X-\alpha_j)^2 + b^i(X-\alpha_j) + c^i)L_j^3,$$

where $0 \leq i \leq 2$. Sparing the readers some (tedious) computations, we find:

$$\begin{aligned}H_j^0(X) &= \Big(\big(6(\mathrm{D}L_j(\alpha_j))^2 - \frac{3}{2}\mathrm{D}^2L_j(\alpha_j)\big)(X-\alpha_j)^2 - 3\mathrm{D}L_j(\alpha_j)(X-\alpha_j) + 1\Big)L_j^3(X),\\ H_j^1(X) &= \Big(9(\mathrm{D}L_j(\alpha_j))^2(X-\alpha_j)^2 - 3\mathrm{D}L_j(\alpha_j)(X-\alpha_j)\Big)L_j^3(X),\\ H_j^2(X) &= \frac{1}{2}(X-\alpha_j)^2L_j^3(X).\end{aligned}$$

Going back to the general problem, it seems to us that a kind of Newton interpolant will be more manageable. Let

$$\begin{aligned}&P_0^0(X) = 1,\\ &P_j^0(X) = (X-\alpha_1)^{n_1+1}\cdots(X-\alpha_j)^{n_j+1},\ \ 1 \leq j \leq m\\ &P_0^i(X) = (X-\alpha_1)^i(X-\alpha_2)^{n_2+1}\cdots(X-\alpha_{m+1})^{n_{m+1}+1},\ \ 1 \leq i \leq n_1,\\ &P_j^i(X) = (X-\alpha_1)^{n_1+1}\cdots(X-\alpha_j)^{n_j+1}(X-\alpha_{j+1})^i(X-\alpha_{j+2})^{n_{j+2}+1}\cdots(X-\alpha_{m+1})^{n_{m+1}+1},\\ &\qquad 1 \leq j \leq m-1,\ 1 \leq i \leq n_{j+1},\\ &P_m^i(X) = (X-\alpha_1)^{n_1+1}\cdots(X-\alpha_m)^{n_m+1}(X-\alpha_{m+1})^i,\ \ 1 \leq i \leq n_{m+1},\end{aligned}$$

and let

$$P(X) = \sum_{j=0,i=0}^{j=m,i=n_{j+1}} \lambda_j^i P_j^i(X).$$

We can think of $P(X)$ as a generalized Newton interpolant. We can compute the derivatives $\mathrm{D}^k P_j^i$, for $1 \leq k \leq n_{j+1}$, and if we look for the Hermite basis polynomials $H_j^i(X)$ such that $\mathrm{D}^i H_j^i(\alpha_j) = 1$ and $\mathrm{D}^k H_j^i(\alpha_l) = 0$, for $k \neq i$ or $l \neq j$, $1 \leq j, l \leq m+1$, $0 \leq i, k \leq n_j$, we find that we have to solve triangular systems of linear equations. Thus, as in the simple case $n_1 = \ldots = n_{m+1} = 0$, we can solve successively for the λ_j^i. Obviously, the computations are quite formidable and we leave such considerations for further study.

Chapter 31

Annihilating Polynomials and the Primary Decomposition

In this chapter all vector spaces are defined over an arbitrary field K.

In Section 7.7 we explained that if $f\colon E \to E$ is a linear map on a K-vector space E, then for any polynomial $p(X) = a_0X^d + a_1X^{d-1} + \cdots + a_d$ with coefficients in the field K, we can define the *linear map* $p(f)\colon E \to E$ by

$$p(f) = a_0f^d + a_1f^{d-1} + \cdots + a_d\mathrm{id},$$

where $f^k = f \circ \cdots \circ f$, the k-fold composition of f with itself. Note that

$$p(f)(u) = a_0f^d(u) + a_1f^{d-1}(u) + \cdots + a_du,$$

for every vector $u \in E$. Then we showed that if E is finite-dimensional and if $\chi_f(X) = \det(XI - f)$ is the characteristic polynomial of f, by the Cayley–Hamilton theorem, we have

$$\chi_f(f) = 0.$$

This fact suggests looking at the set of all polynomials $p(X)$ such that

$$p(f) = 0.$$

Such polynomials are called *annihilating polynomials* of f, the set of all these polynomials, denoted $\mathrm{Ann}(f)$, is called the *annihilator* of f, and the Cayley-Hamilton theorem shows that it is nontrivial since it contains a polynomial of positive degree. It turns out that $\mathrm{Ann}(f)$ contains a polynomial m_f of smallest degree that generates $\mathrm{Ann}(f)$, and this polynomial divides the characteristic polynomial. Furthermore, the polynomial m_f encapsulates a lot of information about f, in particular whether f can be diagonalized. One of the main reasons for this is that a scalar $\lambda \in K$ is a zero of the minimal polynomial m_f if and only if λ is an eigenvalue of f.

The first main result is Theorem 31.6 which states that if $f\colon E \to E$ is a linear map on a finite-dimensional space E, then f is diagonalizable iff its minimal polynomial m is of the form

$$m = (X - \lambda_1) \cdots (X - \lambda_k),$$

where $\lambda_1, \ldots, \lambda_k$ are distinct elements of K.

One of the technical tools used to prove this result is the notion of *f-conductor*; see Definition 31.2. As a corollary of Theorem 31.6 we obtain results about finite commuting families of diagonalizable or triangulable linear maps.

If $f\colon E \to E$ is a linear map and $\lambda \in K$ is an eigenvalue of f, recall that the eigenspace E_λ associated with λ is the kernel of the linear map $\lambda \mathrm{id} - f$. If all the eigenvalues $\lambda_1 \ldots, \lambda_k$ of f are in K and if f is diagonalizable, then

$$E = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_k},$$

but in general there are not enough eigenvectors to span E. A remedy is to generalize the notion of eigenvector and look for (nonzero) vectors u (called generalized eigenvectors) such that

$$(\lambda \mathrm{id} - f)^r(u) = 0, \quad \text{for some } r \geq 1.$$

Then, it turns out that if the minimal polynomial of f is of the form

$$m = (X - \lambda_1)^{r_1} \cdots (X - \lambda_k)^{r_k},$$

then $r = r_i$ does the job for λ_i; that is, if we let

$$W_i = \mathrm{Ker}\,(\lambda_i \mathrm{id} - f)^{r_i},$$

then

$$E = W_1 \oplus \cdots \oplus W_k.$$

The above facts are parts of the *primary decomposition theorem* (Theorem 31.11). It is a special case of a more general result involving the factorization of the minimal polynomial m into its irreducible monic factors; see Theorem 31.10.

Theorem 31.11 implies that every linear map f that has all its eigenvalues in K can be written as $f = D + N$, where D is diagonalizable and N is nilpotent (which means that $N^r = 0$ for some positive integer r). Furthermore D and N commute and are unique. This is the *Jordan decomposition*, Theorem 31.12.

The Jordan decomposition suggests taking a closer look at nilpotent maps. We prove that for any nilpotent linear map $f\colon E \to E$ on a finite-dimensional vector space E of dimension n over a field K, there is a basis of E such that the matrix N of f is of the form

$$N = \begin{pmatrix} 0 & \nu_1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \nu_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & \nu_n \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix},$$

where $\nu_i = 1$ or $\nu_i = 0$; see Theorem 31.16. As a corollary we obtain the *Jordan form*; which involves matrices of the form

$$J_r(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & 1 \\ 0 & 0 & 0 & \cdots & \lambda \end{pmatrix},$$

called *Jordan blocks*; see Theorem 31.17.

31.1 Annihilating Polynomials and the Minimal Polynomial

Given a linear map $f\colon E \to E$, it is easy to check that the set $\mathrm{Ann}(f)$ of polynomials that annihilate f is an ideal. Furthermore, when E is finite-dimensional, the Cayley–Hamilton Theorem implies that $\mathrm{Ann}(f)$ is not the zero ideal. Therefore, by Proposition 30.10, there is a unique monic polynomial m_f that generates $\mathrm{Ann}(f)$. Results from Chapter 30, especially about gcd's of polynomials, will come handy.

Definition 31.1. If $f\colon E \to E$ is a linear map on a finite-dimensional vector space E, the unique monic polynomial $m_f(X)$ that generates the ideal $\mathrm{Ann}(f)$ of polynomials which annihilate f (the *annihilator* of f) is called the *minimal polynomial* of f.

The minimal polynomial m_f of f is the monic polynomial of smallest degree that annihilates f. Thus, the minimal polynomial divides the characteristic polynomial χ_f, and $\deg(m_f) \geq 1$. For simplicity of notation, we often write m instead of m_f.

If A is any $n \times n$ matrix, the set $\mathrm{Ann}(A)$ of polynomials that annihilate A is the set of polynomials

$$p(X) = a_0X^d + a_1X^{d-1} + \cdots + a_{d-1}X + a_d$$

such that

$$a_0A^d + a_1A^{d-1} + \cdots + a_{d-1}A + a_dI = 0.$$

It is clear that $\mathrm{Ann}(A)$ is a nonzero ideal and its unique monic generator is called the *minimal polynomial* of A. We check immediately that if Q is an invertible matrix, then A and $Q^{-1}AQ$ have the same minimal polynomial. Also, if A is the matrix of f with respect to some basis, then f and A have the same minimal polynomial.

The zeros (in K) of the minimal polynomial of f and the eigenvalues of f (in K) are intimately related.

Proposition 31.1. *Let $f\colon E \to E$ be a linear map on some finite-dimensional vector space E. Then $\lambda \in K$ is a zero of the minimal polynomial $m_f(X)$ of f iff λ is an eigenvalue of f*

iff λ is a zero of $\chi_f(X)$. Therefore, the minimal and the characteristic polynomials have the same zeros (in K), except for multiplicities.

Proof. First assume that $m(\lambda) = 0$ (with $\lambda \in K$, and writing m instead of m_f). If so, using polynomial division, m can be factored as

$$m = (X - \lambda)q,$$

with $\deg(q) < \deg(m)$. Since m is the minimal polynomial, $q(f) \neq 0$, so there is some nonzero vector $v \in E$ such that $u = q(f)(v) \neq 0$. But then, because m is the minimal polynomial,

$$\begin{aligned} 0 &= m(f)(v) \\ &= (f - \lambda \mathrm{id})(q(f)(v)) \\ &= (f - \lambda \mathrm{id})(u), \end{aligned}$$

which shows that λ is an eigenvalue of f.

Conversely, assume that $\lambda \in K$ is an eigenvalue of f. This means that for some $u \neq 0$, we have $f(u) = \lambda u$. Now it is easy to show that

$$m(f)(u) = m(\lambda)u,$$

and since m is the minimal polynomial of f, we have $m(f)(u) = 0$, so $m(\lambda)u = 0$, and since $u \neq 0$, we must have $m(\lambda) = 0$. □

Proposition 31.2. *Let $f \colon E \to E$ be a linear map on some finite-dimensional vector space E. If f diagonalizable, then its minimal polynomial is a product of distinct factors of degree 1.*

Proof. If we assume that f is diagonalizable, then its eigenvalues are all in K, and if $\lambda_1, \ldots, \lambda_k$ are the distinct eigenvalues of f, and then by Proposition 31.1, the minimal polynomial m of f must be a product of powers of the polynomials $(X - \lambda_i)$. Actually, we claim that

$$m = (X - \lambda_1) \cdots (X - \lambda_k).$$

For this we just have to show that m annihilates f. However, for any eigenvector u of f, one of the linear maps $f - \lambda_i \mathrm{id}$ sends u to 0, so

$$m(f)(u) = (f - \lambda_1 \mathrm{id}) \circ \cdots \circ (f - \lambda_k \mathrm{id})(u) = 0.$$

Since E is spanned by the eigenvectors of f, we conclude that

$$m(f) = 0.$$ □

It turns out that the converse of Proposition 31.2 is true, but this will take a little work to establish it.

31.2 Minimal Polynomials of Diagonalizable Linear Maps

In this section we prove that if the minimal polynomial m_f of a linear map f is of the form

$$m_f = (X - \lambda_1) \cdots (X - \lambda_k)$$

for distinct scalars $\lambda_1, \ldots, \lambda_k \in K$, then f is diagonalizable. This is a powerful result that has a number of implications. But first we need of few properties of invariant subspaces.

Given a linear map $f \colon E \to E$, recall that a subspace W of E is *invariant under* f if $f(u) \in W$ for all $u \in W$. For example, if $f \colon \mathbb{R}^2 \to \mathbb{R}^2$ is $f(x, y) = (-x, y)$, the y-axis is invariant under f.

Proposition 31.3. *Let W be a subspace of E invariant under the linear map $f \colon E \to E$ (where E is finite-dimensional). Then the minimal polynomial of the restriction $f \mid W$ of f to W divides the minimal polynomial of f, and the characteristic polynomial of $f \mid W$ divides the characteristic polynomial of f.*

Sketch of proof. The key ingredient is that we can pick a basis $(e_1, \ldots, e_n)$ of E in which $(e_1, \ldots, e_k)$ is a basis of W. The matrix of f over this basis is a block matrix of the form

$$A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix},$$

where B is a $k \times k$ matrix, D is an $(n-k) \times (n-k)$ matrix, and C is a $k \times (n-k)$ matrix. Then

$$\det(XI - A) = \det(XI - B)\det(XI - D),$$

which implies the statement about the characteristic polynomials. Furthermore,

$$A^i = \begin{pmatrix} B^i & C_i \\ 0 & D^i \end{pmatrix},$$

for some $k \times (n-k)$ matrix C_i. It follows that any polynomial which annihilates A also annihilates B and D. So the minimal polynomial of B divides the minimal polynomial of A. □

For the next step, there are at least two ways to proceed. We can use an old-fashion argument using Lagrange interpolants, or we can use a slight generalization of the notion of annihilator. We pick the second method because it illustrates nicely the power of principal ideals.

What we need is the notion of conductor (also called transporter).

Definition 31.2. Let $f \colon E \to E$ be a linear map on a finite-dimensional vector space E, let W be an invariant subspace of f, and let u be any vector in E. The set $S_f(u, W)$ consisting of all polynomials $q \in K[X]$ such that $q(f)(u) \in W$ is called the *f-conductor of u into W*.

Observe that the minimal polynomial m_f of f always belongs to $S_f(u, W)$, so this is a nontrivial set. Also, if $W = (0)$, then $S_f(u, (0))$ is just the annihilator of f. The crucial property of $S_f(u, W)$ is that it is an ideal.

Proposition 31.4. *If W is an invariant subspace for f, then for each $u \in E$, the f-conductor $S_f(u, W)$ is an ideal in $K[X]$.*

We leave the proof as a simple exercise, using the fact that if W invariant under f, then W is invariant under every polynomial $q(f)$ in $S_f(u, W)$.

Since $S_f(u, W)$ is an ideal, it is generated by a unique monic polynomial q of smallest degree, and because the minimal polynomial m_f of f is in $S_f(u, W)$, the polynomial q divides m.

Definition 31.3. The unique monic polynomial which generates $S_f(u, W)$ is called the *conductor of u into W*.

Example 31.1. For example, suppose $f \colon \mathbb{R}^2 \to \mathbb{R}^2$ where $f(x, y) = (x, 0)$. Observe that $W = \{(x, 0) \in \mathbb{R}^2\}$ is invariant under f. By representing f as $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, we see that $m_f(X) = \chi_f(X) = X^2 - X$. Let $u = (0, y)$. Then $S_f(u, W) = (X)$ and we say X is the conductor of u into W.

Proposition 31.5. *Let $f \colon E \to E$ be a linear map on a finite-dimensional space E and assume that the minimal polynomial m of f is of the form*

$$m = (X - \lambda_1)^{r_1} \cdots (X - \lambda_k)^{r_k},$$

where the eigenvalues $\lambda_1, \ldots, \lambda_k$ of f belong to K. If W is a proper subspace of E which is invariant under f, then there is a vector $u \in E$ with the following properties:

(a) $u \notin W$;

(b) $(f - \lambda \mathrm{id})(u) \in W$, for some eigenvalue λ of f.

Proof. Observe that (a) and (b) together assert that the conductor of u into W is a polynomial of the form $X - \lambda_i$. Pick any vector $v \in E$ not in W, and let g be the conductor of v into W, i.e. $g(f)(v) \in W$. Since g divides m and $v \notin W$, the polynomial g is not a constant, and thus it is of the form

$$g = (X - \lambda_1)^{s_1} \cdots (X - \lambda_k)^{s_k},$$

with at least some $s_i > 0$. Choose some index j such that $s_j > 0$. Then $X - \lambda_j$ is a factor of g, so we can write

$$g = (X - \lambda_j)q. \tag{*}$$

By definition of g, the vector $u = q(f)(v)$ cannot be in W, since otherwise g would not be of minimal degree. However, $(*)$ implies that

$$\begin{aligned}(f - \lambda_j \mathrm{id})(u) &= (f - \lambda_j \mathrm{id})(q(f)(v)) \\ &= g(f)(v)\end{aligned}$$

is in W, which concludes the proof. □

We can now prove the main result of this section.

Theorem 31.6. *Let $f \colon E \to E$ be a linear map on a finite-dimensional space E. Then f is diagonalizable iff its minimal polynomial m is of the form*

$$m = (X - \lambda_1) \cdots (X - \lambda_k),$$

where $\lambda_1, \ldots, \lambda_k$ are distinct elements of K.

Proof. We already showed in Proposition 31.2 that if f is diagonalizable, then its minimal polynomial is of the above form (where $\lambda_1, \ldots, \lambda_k$ are the distinct eigenvalues of f).

For the converse, let W be the subspace spanned by all the eigenvectors of f. If $W \neq E$, since W is invariant under f, by Proposition 31.5, there is some vector $u \notin W$ such that for some λ_j, we have

$$(f - \lambda_j \mathrm{id})(u) \in W.$$

Let $v = (f - \lambda_j \mathrm{id})(u) \in W$. Since $v \in W$, we can write

$$v = w_1 + \cdots + w_k$$

where $f(w_i) = \lambda_i w_i$ (either $w_i = 0$ or w_i is an eigenvector for λ_i), and so for every polynomial h, we have

$$h(f)(v) = h(\lambda_1) w_1 + \cdots + h(\lambda_k) w_k,$$

which shows that $h(f)(v) \in W$ for every polynomial h. We can write

$$m = (X - \lambda_j) q$$

for some polynomial q, and also

$$q - q(\lambda_j) = p(X - \lambda_j)$$

for some polynomial p. We know that $p(f)(v) \in W$, and since m is the minimal polynomial of f, we have

$$0 = m(f)(u) = (f - \lambda_j \mathrm{id})(q(f)(u)),$$

which implies that $q(f)(u) \in W$ (either $q(f)(u) = 0$, or it is an eigenvector associated with λ_j). However,

$$q(f)(u) - q(\lambda_j) u = p(f)((f - \lambda_j \mathrm{id})(u)) = p(f)(v),$$

and since $p(f)(v) \in W$ and $q(f)(u) \in W$, we conclude that $q(\lambda_j) u \in W$. But, $u \notin W$, which implies that $q(\lambda_j) = 0$, so λ_j is a double root of m, a contradiction. Therefore, we must have $W = E$. □

Remark: Proposition 31.5 can be used to give a quick proof of Theorem 15.5.

31.3 Commuting Families of Diagonalizable and Triangulable Maps

Using Theorem 31.6, we can give a short proof about commuting diagonalizable linear maps.

Definition 31.4. If $\mathcal{F}$ is a family of linear maps on a vector space E, we say that $\mathcal{F}$ is a *commuting family* iff $f \circ g = g \circ f$ for all $f, g \in \mathcal{F}$.

Proposition 31.7. *Let $\mathcal{F}$ be a finite commuting family of diagonalizable linear maps on a vector space E. There exists a basis of E such that every linear map in $\mathcal{F}$ is represented in that basis by a diagonal matrix.*

Proof. We proceed by induction on $n = \dim(E)$. If $n = 1$, there is nothing to prove. If $n > 1$, there are two cases. If all linear maps in $\mathcal{F}$ are of the form $\lambda\mathrm{id}$ for some $\lambda \in K$, then the proposition holds trivially. In the second case, let $f \in \mathcal{F}$ be some linear map in $\mathcal{F}$ which is not a scalar multiple of the identity. In this case, f has at least two distinct eigenvalues $\lambda_1, \ldots, \lambda_k$, and because f is diagonalizable, E is the direct sum of the corresponding eigenspaces $E_{\lambda_1}, \ldots, E_{\lambda_k}$. For every index i, the eigenspace E_{λ_i} is invariant under f and under every other linear map g in $\mathcal{F}$, since for any $g \in \mathcal{F}$ and any $u \in E_{\lambda_i}$, because f and g commute, we have

$$f(g(u)) = g(f(u)) = g(\lambda_i u) = \lambda_i g(u)$$

so $g(u) \in E_{\lambda_i}$. Let $\mathcal{F}_i$ be the family obtained by restricting each $f \in \mathcal{F}$ to E_{λ_i}. By Proposition 31.3, the minimal polynomial of every linear map $f \mid E_{\lambda_i}$ in $\mathcal{F}_i$ divides the minimal polynomial m_f of f, and since f is diagonalizable, m_f is a product of distinct linear factors, so the minimal polynomial of $f \mid E_{\lambda_i}$ is also a product of distinct linear factors. By Theorem 31.6, the linear map $f \mid E_{\lambda_i}$ is diagonalizable. Since $k > 1$, we have $\dim(E_{\lambda_i}) < \dim(E)$ for $i = 1, \ldots, k$, and by the induction hypothesis, for each i there is a basis of E_{λ_i} over which $f \mid E_{\lambda_i}$ is represented by a diagonal matrix. Since the above argument holds for all i, by combining the bases of the E_{λ_i}, we obtain a basis of E such that the matrix of every linear map $f \in \mathcal{F}$ is represented by a diagonal matrix. □

Remark: Proposition 31.7 also holds for infinite commuting families $\mathcal{F}$ of diagonalizable linear maps, because E being finite dimensional, there is a finite subfamily of linearly independent linear maps in $\mathcal{F}$ spanning $\mathcal{F}$.

There is also an analogous result for commuting families of linear maps represented by upper triangular matrices. To prove this we need the following proposition.

Proposition 31.8. *Let $\mathcal{F}$ be a nonempty finite commuting family of triangulable linear maps on a finite-dimensional vector space E. Let W be a proper subspace of E which is invariant under $\mathcal{F}$. Then there exists a vector $u \in E$ such that:*

1. $u \notin W$.

2. For every $f \in \mathcal{F}$, the vector $f(u)$ belongs to the subspace $W \oplus Ku$ spanned by W and u.

Proof. By renaming the elements of $\mathcal{F}$ if necessary, we may assume that $(f_1, \ldots, f_r)$ is a basis of the subspace of $\mathrm{End}(E)$ spanned by $\mathcal{F}$. We prove by induction on r that there exists some vector $u \in E$ such that

1. $u \notin W$.
2. $(f_i - \alpha_i \mathrm{id})(u) \in W$ for $i = 1, \ldots, r$, for some scalars $\alpha_i \in K$.

Consider the base case $r = 1$. Since f_1 is triangulable, its eigenvalues all belong to K since they are the diagonal entries of the triangular matrix associated with f_1 (this is the easy direction of Theorem 15.5), so the minimal polynomial of f_1 is of the form

$$m = (X - \lambda_1)^{r_1} \cdots (X - \lambda_k)^{r_k},$$

where the eigenvalues $\lambda_1, \ldots, \lambda_k$ of f_1 belong to K. We conclude by applying Proposition 31.5.

Next assume that $r \geq 2$ and that the induction hypothesis holds for $f_1, \ldots, f_{r-1}$. Thus, there is a vector $u_{r-1} \in E$ such that

1. $u_{r-1} \notin W$.
2. $(f_i - \alpha_i \mathrm{id})(u_{r-1}) \in W$ for $i = 1, \ldots, r-1$, for some scalars $\alpha_i \in K$.

Let

$$V_{r-1} = \{w \in E \mid (f_i - \alpha_i \mathrm{id})(w) \in W,\ i = 1, \ldots, r-1\}.$$

Clearly, $W \subseteq V_{r-1}$ and $u_{r-1} \in V_{r-1}$. We claim that V_{r-1} is invariant under $\mathcal{F}$. This is because, for any $v \in V_{r-1}$ and any $f \in \mathcal{F}$, since f and f_i commute, we have

$$(f_i - \alpha_i \mathrm{id})(f(v)) = f((f_i - \alpha_i \mathrm{id})(v)), \quad 1 \leq i \leq r-1.$$

Now $(f_i - \alpha_i \mathrm{id})(v) \in W$ because $v \in V_{r-1}$, and W is invariant under $\mathcal{F}$, so $f(f_i - \alpha_i \mathrm{id})(v)) \in W$, that is, $(f_i - \alpha_i \mathrm{id})(f(v)) \in W$.

Consider the restriction g_r of f_r to V_{r-1}. The minimal polynomial of g_r divides the minimal polynomial of f_r, and since f_r is triangulable, just as we saw for f_1, the minimal polynomial of f_r is of the form

$$m = (X - \lambda_1)^{r_1} \cdots (X - \lambda_k)^{r_k},$$

where the eigenvalues $\lambda_1, \ldots, \lambda_k$ of f_r belong to K, so the minimal polynomial of g_r is of the same form. By Proposition 31.5, there is some vector $u_r \in V_{r-1}$ such that

1. $u_r \notin W$.

2. $(g_r - \alpha_r \mathrm{id})(u_r) \in W$ for some scalars $\alpha_r \in K$.

Now since $u_r \in V_{r-1}$, we have $(f_i - \alpha_i \mathrm{id})(u_r) \in W$ for $i = 1, \ldots, r-1$, so $(f_i - \alpha_i \mathrm{id})(u_r) \in W$ for $i = 1, \ldots, r$ (since g_r is the restriction of f_r), which concludes the proof of the induction step. Finally, since every $f \in \mathcal{F}$ is the linear combination of $(f_1, \ldots, f_r)$, Condition (2) of the inductive claim implies Condition (2) of the proposition. □

We can now prove the following result.

Proposition 31.9. *Let $\mathcal{F}$ be a nonempty finite commuting family of triangulable linear maps on a finite-dimensional vector space E. There exists a basis of E such that every linear map in $\mathcal{F}$ is represented in that basis by an upper triangular matrix.*

Proof. Let $n = \dim(E)$. We construct inductively a basis $(u_1, \ldots, u_n)$ of E such that if W_i is the subspace spanned by $(u_1 \ldots, u_i)$, then for every $f \in \mathcal{F}$,

$$f(u_i) = a^f_{1i} u_1 + \cdots + a^f_{ii} u_i,$$

for some $a^f_{ij} \in K$; that is, $f(u_i)$ belongs to the subspace W_i.

We begin by applying Proposition 31.8 to the subspace $W_0 = (0)$ to get u_1 so that for all $f \in \mathcal{F}$,

$$f(u_1) = \alpha^f_1 u_1.$$

For the induction step, since W_i invariant under $\mathcal{F}$, we apply Proposition 31.8 to the subspace W_i, to get $u_{i+1} \in E$ such that

1. $u_{i+1} \notin W_i$.

2. For every $f \in \mathcal{F}$, the vector $f(u_{i+1})$ belong to the subspace spanned by W_i and u_{i+1}.

Condition (1) implies that $(u_1, \ldots, u_i, u_{i+1})$ is linearly independent, and Condition (2) means that for every $f \in \mathcal{F}$,

$$f(u_{i+1}) = a^f_{1i+1} u_1 + \cdots + a^f_{i+1i+1} u_{i+1},$$

for some $a^f_{i+1j} \in K$, establishing the induction step. After n steps, each $f \in \mathcal{F}$ is represented by an upper triangular matrix. □

Observe that if $\mathcal{F}$ consists of a single linear map f and if the minimal polynomial of f is of the form

$$m = (X - \lambda_1)^{r_1} \cdots (X - \lambda_k)^{r_k},$$

with all $\lambda_i \in K$, using Proposition 31.5 instead of Proposition 31.8, the proof of Proposition 31.9 yields another proof of Theorem 15.5.

31.4 The Primary Decomposition Theorem

If $f\colon E \to E$ is a linear map and $\lambda \in K$ is an eigenvalue of f, recall that the eigenspace E_λ associated with λ is the kernel of the linear map $\lambda\mathrm{id} - f$. If all the eigenvalues $\lambda_1 \ldots, \lambda_k$ of f are in K, it may happen that

$$E = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_k},$$

but in general there are not enough eigenvectors to span E. What if we generalize the notion of eigenvector and look for (nonzero) vectors u such that

$$(\lambda\mathrm{id} - f)^r(u) = 0, \quad \text{for some } r \geq 1?$$

It turns out that if the minimal polynomial of f is of the form

$$m = (X - \lambda_1)^{r_1} \cdots (X - \lambda_k)^{r_k},$$

then $r = r_i$ does the job for λ_i; that is, if we let

$$W_i = \mathrm{Ker}\,(\lambda_i\mathrm{id} - f)^{r_i},$$

then

$$E = W_1 \oplus \cdots \oplus W_k.$$

This result is very nice but seems to require that the eigenvalues of f all belong to K. Actually, it is a special case of a more general result involving the factorization of the minimal polynomial m into its irreducible monic factors (see Theorem 30.17),

$$m = p_1^{r_1} \cdots p_k^{r_k},$$

where the p_i are distinct irreducible monic polynomials over K.

Theorem 31.10. *(Primary Decomposition Theorem) Let $f\colon E \to E$ be a linear map on the finite-dimensional vector space E over the field K. Write the minimal polynomial m of f as*

$$m = p_1^{r_1} \cdots p_k^{r_k},$$

where the p_i are distinct irreducible monic polynomials over K, and the r_i are positive integers. Let

$$W_i = \mathrm{Ker}\,(p_i^{r_i}(f)), \quad i = 1, \ldots, k.$$

Then

(a) $E = W_1 \oplus \cdots \oplus W_k$.

(b) Each W_i is invariant under f.

(c) The minimal polynomial of the restriction $f \mid W_i$ of f to W_i is $p_i^{r_i}$.

Proof. The trick is to construct projections π_i using the polynomials $p_j^{r_j}$ so that the range of π_i is equal to W_i. Let

$$g_i = m/p_i^{r_i} = \prod_{j \neq i} p_j^{r_j}.$$

Note that

$$p_i^{r_i} g_i = m.$$

Since $p_1, \ldots, p_k$ are irreducible and distinct, they are relatively prime. Then using Proposition 30.14, it is easy to show that $g_1, \ldots, g_k$ are relatively prime. Otherwise, some irreducible polynomial p would divide all of $g_1, \ldots, g_k$, so by Proposition 30.14 it would be equal to one of the irreducible factors p_i. But that p_i is missing from g_i, a contradiction. Therefore, by Proposition 30.15, there exist some polynomials $h_1, \ldots, h_k$ such that

$$g_1 h_1 + \cdots + g_k h_k = 1.$$

Let $q_i = g_i h_i$ and let $\pi_i = q_i(f) = g_i(f) h_i(f)$. We have

$$q_1 + \cdots + q_k = 1,$$

and since m divides $q_i q_j$ for $i \neq j$, we get

$$\begin{aligned} \pi_1 + \cdots + \pi_k &= \mathrm{id} \\ \pi_i \pi_j &= 0, \quad i \neq j. \end{aligned}$$

(We implicitly used the fact that if p, q are two polynomials, the linear maps $p(f) \circ q(f)$ and $q(f) \circ p(f)$ are the same since $p(f)$ and $q(f)$ are polynomials in the powers of f, which commute.) Composing the first equation with π_i and using the second equation, we get

$$\pi_i^2 = \pi_i.$$

Therefore, the π_i are projections, and E is the direct sum of the images of the π_i. Indeed, every $u \in E$ can be expressed as

$$u = \pi_1(u) + \cdots + \pi_k(u).$$

Also, if

$$\pi_1(u) + \cdots + \pi_k(u) = 0,$$

then by applying π_i we get

$$0 = \pi_i^2(u) = \pi_i(u), \quad i = 1, \ldots k.$$

To finish proving (a), we need to show that

$$W_i = \mathrm{Ker}\,(p_i^{r_i}(f)) = \pi_i(E).$$

If $v \in \pi_i(E)$, then $v = \pi_i(u)$ for some $u \in E$, so

$$\begin{aligned} p_i^{r_i}(f)(v) &= p_i^{r_i}(f)(\pi_i(u)) \\ &= p_i^{r_i}(f)g_i(f)h_i(f)(u) \\ &= h_i(f)p_i^{r_i}(f)g_i(f)(u) \\ &= h_i(f)m(f)(u) = 0, \end{aligned}$$

because m is the minimal polynomial of f. Therefore, $v \in W_i$.

Conversely, assume that $v \in W_i = \mathrm{Ker}\,(p_i^{r_i}(f))$. If $j \neq i$, then g_jh_j is divisible by $p_i^{r_i}$, so

$$g_j(f)h_j(f)(v) = \pi_j(v) = 0, \quad j \neq i.$$

Then since $\pi_1 + \cdots + \pi_k = \mathrm{id}$, we have $v = \pi_i v$, which shows that v is in the range of π_i. Therefore, $W_i = \mathrm{Im}(\pi_i)$, and this finishes the proof of (a).

If $p_i^{r_i}(f)(u) = 0$, then $p_i^{r_i}(f)(f(u)) = f(p_i^{r_i}(f)(u)) = 0$, so (b) holds.

If we write $f_i = f \mid W_i$, then $p_i^{r_i}(f_i) = 0$, because $p_i^{r_i}(f) = 0$ on W_i (its kernel). Therefore, the minimal polynomial of f_i divides $p_i^{r_i}$. Conversely, let q be any polynomial such that $q(f_i) = 0$ (on W_i). Since $m = p_i^{r_i}g_i$, the fact that $m(f)(u) = 0$ for all $u \in E$ shows that

$$p_i^{r_i}(f)(g_i(f)(u)) = 0, \quad u \in E,$$

and thus $\mathrm{Im}(g_i(f)) \subseteq \mathrm{Ker}\,(p_i^{r_i}(f)) = W_i$. Consequently, since $q(f)$ is zero on W_i,

$$q(f)g_i(f) = 0 \quad \text{for all } u \in E.$$

But then qg_i is divisible by the minimal polynomial $m = p_i^{r_i}g_i$ of f, and since $p_i^{r_i}$ and g_i are relatively prime, by Euclid's proposition, $p_i^{r_i}$ must divide q. This finishes the proof that the minimal polynomial of f_i is $p_i^{r_i}$, which is (c). □

To best understand the projection constructions of Theorem 31.10, we provide the following two explicit examples of the primary decomposition theorem.

Example 31.2. First let $f\colon \mathbb{R}^3 \to \mathbb{R}^3$ be defined as $f(x, y, z) = (y, -x, z)$. In terms of the standard basis f is represented by the 3×3 matrix $X_f := \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Then a simple calculation shows that $m_f(x) = \chi_f(x) = (x^2+1)(x-1)$. Using the notation of the preceding proof set

$$m = p_1p_2, \qquad p_1 = x^2 + 1, \qquad p_2 = x - 1.$$

Then

$$g_1 = \frac{m}{p_1} = x - 1, \qquad g_2 = \frac{m}{p_2} = x^2 + 1.$$

We must find $h_1, h_2 \in \mathbb{R}[x]$ such that $g_1 h_1 + g_2 h_2 = 1$. In general this is the hard part of the projection construction. But since we are only working with two relatively prime polynomials g_1, g_2, we may apply the Euclidean algorithm to discover that

$$-\frac{x+1}{2}(x-1) + \frac{1}{2}(x^2+1) = 1,$$

where $h_1 = -\frac{x+1}{2}$ while $h_2 = \frac{1}{2}$. By definition

$$\pi_1 = g_1(f)h_1(f) = -\frac{1}{2}(X_f - \mathrm{id})(X_f + \mathrm{id}) = -\frac{1}{2}(X_f^2 - \mathrm{id}) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

and

$$\pi_2 = g_2(f)h_2(f) = \frac{1}{2}(X_f^2 + \mathrm{id}) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then $\mathbb{R}^3 = W_1 \oplus W_2$, where

$$W_1 = \pi_1(\mathbb{R}^3) = \mathrm{Ker}\,(p_1(X_f)) = \mathrm{Ker}\,(X_f^2 + \mathrm{id}) = \mathrm{Ker}\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \{(x, y, 0) \in \mathbb{R}^3\},$$

$$W_2 = \pi_2(\mathbb{R}^3) = \mathrm{Ker}\,(p_2(X_f)) = \mathrm{Ker}\,(X_f - \mathrm{id}) = \mathrm{Ker}\begin{pmatrix} -1 & -1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \{(0, 0, z) \in \mathbb{R}^3\}.$$

Example 31.3. For our second example of the primary decomposition theorem let $f\colon \mathbb{R}^3 \to \mathbb{R}^3$ be defined as $f(x, y, z) = (y, -x + z, -y)$, with standard matrix representation $X_f = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$. A simple calculation shows that $m_f(x) = \chi_f(x) = x(x^2 + 2)$. Set

$$p_1 = x^2 + 2, \qquad p_2 = x, \qquad g_1 = \frac{m_f}{p_1} = x, \qquad g_2 = \frac{m_f}{p_2} = x^2 + 2.$$

Since $\gcd(g_1, g_2) = 1$, we use the Euclidean algorithm to find

$$h_1 = -\frac{1}{2}x, \qquad h_2 = \frac{1}{2},$$

such that $g_1 h_1 + g_2 h_2 = 1$. Then

$$\pi_1 = g_1(f)h_1(f) = -\frac{1}{2}X_f^2 = \begin{pmatrix} \frac{1}{2} & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \\ -\frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix},$$

while

$$\pi_2 = g_2(f)h_2(f) = \frac{1}{2}(X_f^2 + 2\mathrm{id}) = \begin{pmatrix} \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 0 & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix}.$$

Although it is not entirely obvious, π_1 and π_2 are indeed projections since

$$\pi_1^2 = \begin{pmatrix} \frac{1}{2} & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \\ -\frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} \frac{1}{2} & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \\ -\frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \\ -\frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix} = \pi_1,$$

and

$$\pi_2^2 = \begin{pmatrix} \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 0 & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 0 & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 0 & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix} = \pi_2.$$

Furthermore observe that $\pi_1 + \pi_2 = \mathrm{id}$. The primary decomposition theorem implies that $\mathbb{R}^3 = W_1 \oplus W_2$ where

$$W_1 = \pi_1(\mathbb{R}^3) = \mathrm{Ker}\,(p_1(f)) = \mathrm{Ker}\,(X^2 + 2) = \mathrm{Ker}\,\begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix} = \mathrm{span}\{(0,1,0),(1,0,-1)\},$$
$$W_2 = \pi_2(\mathbb{R}^3) = \mathrm{Ker}\,(p_2(f)) = \mathrm{Ker}\,(X) = \mathrm{span}\{(1,0,1)\}.$$

See Figure 31.1.

If all the eigenvalues of f belong to the field K, we obtain the following result.

Theorem 31.11. *(Primary Decomposition Theorem, Version 2) Let $f\colon E \to E$ be a linear map on the finite-dimensional vector space E over the field K. If all the eigenvalues $\lambda_1, \ldots, \lambda_k$ of f belong to K, write*

$$m = (X - \lambda_1)^{r_1} \cdots (X - \lambda_k)^{r_k}$$

for the minimal polynomial of f,

$$\chi_f = (X - \lambda_1)^{n_1} \cdots (X - \lambda_k)^{n_k}$$

for the characteristic polynomial of f, with $1 \leq r_i \leq n_i$, and let

$$W_i = \mathrm{Ker}\,(\lambda_i \mathrm{id} - f)^{r_i}, \quad i = 1, \ldots, k.$$

Then

(a) $E = W_1 \oplus \cdots \oplus W_k$.

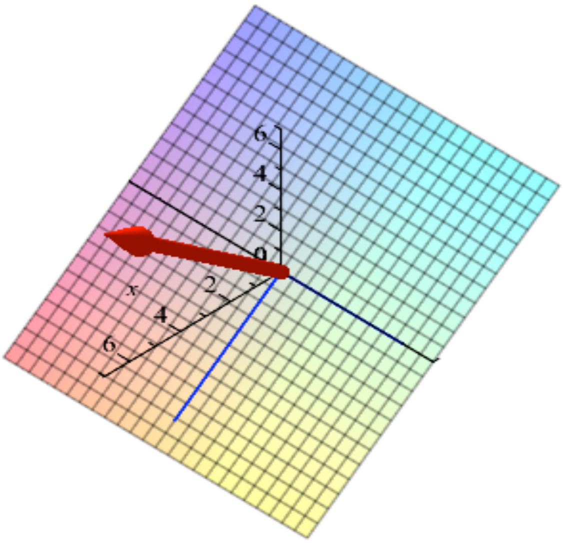

Figure 31.1: The direct sum decomposition of $\mathbb{R}^3 = W_1 \oplus W_2$ where W_1 is the plane $x+z=0$ and W_2 is line $t(1,0,1)$. The spanning vectors of W_1 are in blue.

(b) *Each W_i is invariant under f.*

(c) $\dim(W_i) = n_i$.

(d) *The minimal polynomial of the restriction $f \mid W_i$ of f to W_i is $(X-\lambda_i)^{r_i}$.*

Proof. Parts (a), (b) and (d) have already been proven in Theorem 31.10, so it remains to prove (c). Since W_i is invariant under f, let f_i be the restriction of f to W_i. The characteristic polynomial χ_{f_i} of f_i divides $\chi(f)$, and since $\chi(f)$ has all its roots in K, so does $\chi_i(f)$. By Theorem 15.5, there is a basis of W_i in which f_i is represented by an upper triangular matrix, and since $(\lambda_i \mathrm{id} - f)^{r_i} = 0$, the diagonal entries of this matrix are equal to λ_i. Consequently,

$$\chi_{f_i} = (X-\lambda_i)^{\dim(W_i)},$$

and since χ_{f_i} divides $\chi(f)$, we conclude hat

$$\dim(W_i) \leq n_i, \quad i = 1, \ldots, k.$$

Because E is the direct sum of the W_i, we have $\dim(W_1) + \cdots + \dim(W_k) = n$, and since $n_1 + \cdots + n_k = n$, we must have

$$\dim(W_i) = n_i, \quad i = 1, \ldots, k,$$

proving (c). □

Definition 31.5. If $\lambda \in K$ is an eigenvalue of f, we define a *generalized eigenvector* of f as a nonzero vector $u \in E$ such that

$$(\lambda \mathrm{id} - f)^r(u) = 0, \quad \text{for some } r \geq 1.$$

The *index* of λ is defined as the smallest $r \geq 1$ such that

$$\mathrm{Ker}\,(\lambda \mathrm{id} - f)^r = \mathrm{Ker}\,(\lambda \mathrm{id} - f)^{r+1}.$$

It is clear that $\mathrm{Ker}\,(\lambda \mathrm{id} - f)^i \subseteq \mathrm{Ker}\,(\lambda \mathrm{id} - f)^{i+1}$ for all $i \geq 1$. By Theorem 31.11(d), if $\lambda = \lambda_i$, the index of λ_i is equal to r_i.

31.5 Jordan Decomposition

Recall that a linear map $g\colon E \to E$ is said to be *nilpotent* if there is some positive integer r such that $g^r = 0$. Another important consequence of Theorem 31.11 is that f can be written as the sum of a diagonalizable and a nilpotent linear map (which commute). For example $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ be the $\mathbb{R}$-linear map $f(x, y) = (x, x + y)$ with standard matrix representation $X_f = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. A basic calculation shows that $m_f(x) = \chi_f(x) = (x-1)^2$. By Theorem 31.6 we know that f is not diagonalizable over $\mathbb{R}$. But since the eigenvalue $\lambda_1 = 1$ of f does belong to $\mathbb{R}$, we may use the projection construction inherent within Theorem 31.11 to write $f = D + N$, where D is a diagonalizable linear map and N is a nilpotent linear map. The proof of Theorem 31.10 implies that

$$p_1^{r_1} = (x-1)^2, \qquad g_1 = 1 = h_1, \qquad \pi_1 = g_1(f)h_1(f) = \mathrm{id}.$$

Then

$$D = \lambda_1\pi_1 = \mathrm{id}, \qquad N = f - D = f(x, y) - \mathrm{id}(x, y) = (x, x + y) - (x, y) = (0, y),$$

which is equivalent to the matrix decomposition

$$X_f = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

This example suggests that the diagonal summand of f is related to the projection constructions associated with the proof of the primary decomposition theorem. If we write

$$D = \lambda_1\pi_1 + \cdots + \lambda_k\pi_k,$$

where π_i is the projection from E onto the subspace W_i defined in the proof of Theorem 31.10, since

$$\pi_1 + \cdots + \pi_k = \mathrm{id},$$

we have

$$f = f\pi_1 + \cdots + f\pi_k,$$

and so we get

$$N = f - D = (f - \lambda_1 \mathrm{id})\pi_1 + \cdots + (f - \lambda_k \mathrm{id})\pi_k.$$

We claim that $N = f - D$ is a nilpotent operator. Since by construction the π_i are polynomials in f, they commute with f, using the properties of the π_i, we get

$$N^r = (f - \lambda_1 \mathrm{id})^r \pi_1 + \cdots + (f - \lambda_k \mathrm{id})^r \pi_k.$$

Therefore, if $r = \max\{r_i\}$, we have $(f - \lambda_k \mathrm{id})^r = 0$ for $i = 1, \ldots, k$, which implies that

$$N^r = 0.$$

It remains to show that D is diagonalizable. Since N is a polynomial in f, it commutes with f, and thus with D. From

$$D = \lambda_1\pi_1 + \cdots + \lambda_k\pi_k,$$

and

$$\pi_1 + \cdots + \pi_k = \mathrm{id},$$

we see that

$$\begin{aligned} D - \lambda_i \mathrm{id} &= \lambda_1\pi_1 + \cdots + \lambda_k\pi_k - \lambda_i(\pi_1 + \cdots + \pi_k) \\ &= (\lambda_1 - \lambda_i)\pi_1 + \cdots + (\lambda_{i-1} - \lambda_i)\pi_{i-1} + (\lambda_{i+1} - \lambda_i)\pi_{i+1} + \cdots + (\lambda_k - \lambda_i)\pi_k. \end{aligned}$$

Since the projections π_j with $j \neq i$ vanish on W_i, the above equation implies that $D - \lambda_i \mathrm{id}$ vanishes on W_i and that $(D - \lambda_j \mathrm{id})(W_i) \subseteq W_i$, and thus that the minimal polynomial of D is

$$(X - \lambda_1) \cdots (X - \lambda_k).$$

Since the λ_i are distinct, by Theorem 31.6, the linear map D is diagonalizable.

In summary we have shown that when all the eigenvalues of f belong to K, there exist a diagonalizable linear map D and a nilpotent linear map N such that

$$\begin{aligned} f &= D + N \\ DN &= ND, \end{aligned}$$

and N and D are polynomials in f.

Definition 31.6. A decomposition of f as $f = D + N$ as above is called a *Jordan decomposition.*

In fact, we can prove more: the maps D and N are uniquely determined by f.

Theorem 31.12. *(Jordan Decomposition) Let $f\colon E \to E$ be a linear map on the finite-dimensional vector space E over the field K. If all the eigenvalues $\lambda_1, \ldots, \lambda_k$ of f belong to K, then there exist a diagonalizable linear map D and a nilpotent linear map N such that*

$$\begin{aligned} f &= D + N \\ DN &= ND. \end{aligned}$$

Furthermore, D and N are uniquely determined by the above equations and they are polynomials in f.

Proof. We already proved the existence part. Suppose we also have $f = D' + N'$, with $D'N' = N'D'$, where D' is diagonalizable, N' is nilpotent, and both are polynomials in f. We need to prove that $D = D'$ and $N = N'$.

Since D' and N' commute with one another and $f = D' + N'$, we see that D' and N' commute with f. Then D' and N' commute with any polynomial in f; hence they commute with D and N. From

$$D + N = D' + N',$$

we get

$$D - D' = N' - N,$$

and D, D', N, N' commute with one another. Since D and D' are both diagonalizable and commute, by Proposition 31.7, they are simultaneousy diagonalizable, so $D - D'$ is diagonalizable. Since N and N' commute, by the binomial formula, for any $r \geq 1$,

$$(N' - N)^r = \sum_{j=0}^{r} (-1)^j \binom{r}{j} (N')^{r-j} N^j.$$

Since both N and N' are nilpotent, we have $N^{r_1} = 0$ and $(N')^{r_2} = 0$, for some $r_1, r_2 > 0$, so for $r \geq r_1 + r_2$, the right-hand side of the above expression is zero, which shows that $N' - N$ is nilpotent. (In fact, it is easy that $r_1 = r_2 = n$ works). It follows that $D - D' = N' - N$ is both diagonalizable and nilpotent. Clearly, the minimal polynomial of a nilpotent linear map is of the form X^r for some $r > 0$ (and $r \leq \dim(E)$). But $D - D'$ is diagonalizable, so its minimal polynomial has simple roots, which means that $r = 1$. Therefore, the minimal polynomial of $D - D'$ is X, which says that $D - D' = 0$, and then $N = N'$. □

If K is an algebraically closed field, then Theorem 31.12 holds. This is the case when $K = \mathbb{C}$. This theorem reduces the study of linear maps (from E to itself) to the study of nilpotent operators. There is a special normal form for such operators which is discussed in the next section.

31.6 Nilpotent Linear Maps and Jordan Form

This section is devoted to a normal form for nilpotent maps. We follow Godement's exposition [76]. Let $f\colon E \to E$ be a nilpotent linear map on a finite-dimensional vector space over a field K, and assume that f is not the zero map. There is a smallest positive integer $r \geq 1$ such $f^r \neq 0$ and $f^{r+1} = 0$. Clearly, the polynomial X^{r+1} annihilates f, and it is the minimal polynomial of f since $f^r \neq 0$. It follows that $r + 1 \leq n = \dim(E)$. Let us define the subspaces N_i by

$$N_i = \mathrm{Ker}\,(f^i), \quad i \geq 0.$$

Note that $N_0 = (0)$, $N_1 = \mathrm{Ker}\,(f)$, and $N_{r+1} = E$. Also, it is obvious that

$$N_i \subseteq N_{i+1}, \quad i \geq 0.$$

Proposition 31.13. *Given a nilpotent linear map f with $f^r \neq 0$ and $f^{r+1} = 0$ as above, the inclusions in the following sequence are strict:*

$$(0) = N_0 \subset N_1 \subset \cdots \subset N_r \subset N_{r+1} = E.$$

Proof. We proceed by contradiction. Assume that $N_i = N_{i+1}$ for some i with $0 \leq i \leq r$. Since $f^{r+1} = 0$, for every $u \in E$, we have

$$0 = f^{r+1}(u) = f^{i+1}(f^{r-i}(u)),$$

which shows that $f^{r-i}(u) \in N_{i+1}$. Since $N_i = N_{i+1}$, we get $f^{r-i}(u) \in N_i$, and thus $f^r(u) = 0$. Since this holds for all $u \in E$, we see that $f^r = 0$, a contradiction. □

Proposition 31.14. *Given a nilpotent linear map f with $f^r \neq 0$ and $f^{r+1} = 0$, for any integer i with $1 \leq i \leq r$, for any subspace U of E, if $U \cap N_i = (0)$, then $f(U) \cap N_{i-1} = (0)$, and the restriction of f to U is an isomorphism onto $f(U)$.*

Proof. Pick $v \in f(U) \cap N_{i-1}$. We have $v = f(u)$ for some $u \in U$ and $f^{i-1}(v) = 0$, which means that $f^i(u) = 0$. Then $u \in U \cap N_i$, so $u = 0$ since $U \cap N_i = (0)$, and $v = f(u) = 0$. Therefore, $f(U) \cap N_{i-1} = (0)$. The restriction of f to U is obviously surjective on $f(U)$. Suppose that $f(u) = 0$ for some $u \in U$. Then $u \in U \cap N_1 \subseteq U \cap N_i = (0)$ (since $i \geq 1$), so $u = 0$, which proves that f is also injective on U. □

Proposition 31.15. *Given a nilpotent linear map f with $f^r \neq 0$ and $f^{r+1} = 0$, there exists a sequence of subspace $U_1, \ldots, U_{r+1}$ of E with the following properties:*

(1) $N_i = N_{i-1} \oplus U_i$, for $i = 1, \ldots, r + 1$.

(2) We have $f(U_i) \subseteq U_{i-1}$, and the restriction of f to U_i is an injection, for $i = 2, \ldots, r+1$.

See Figure 31.2.

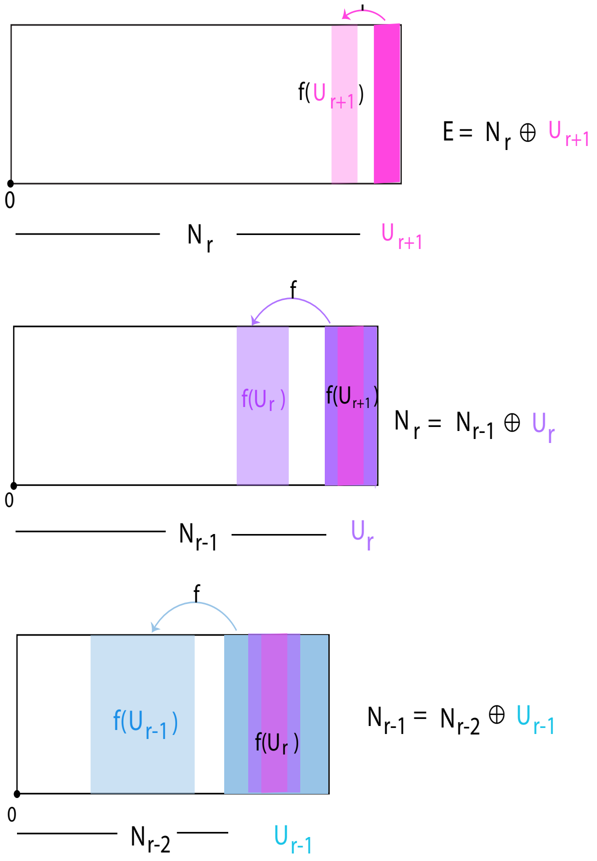

Figure 31.2: A schematic illustration of $N_i = N_{i-1} \oplus U_i$ with $f(U_i) \subseteq U_{i-1}$ for $i = r+1, r, r-1$.

Proof. We proceed inductively, by defining the sequence $U_{r+1}, U_r, \ldots, U_1$. We pick U_{r+1} to be any supplement of N_r in $N_{r+1} = E$, so that

$$E = N_{r+1} = N_r \oplus U_{r+1}.$$

Since $f^{r+1} = 0$ and $N_r = \mathrm{Ker}\,(f^r)$, we have $f(U_{r+1}) \subseteq N_r$, and by Proposition 31.14, as $U_{r+1} \cap N_r = (0)$, we have $f(U_{r+1}) \cap N_{r-1} = (0)$. As a consequence, we can pick a supplement U_r of N_{r-1} in N_r so that $f(U_{r+1}) \subseteq U_r$. We have

$$N_r = N_{r-1} \oplus U_r \quad \text{and} \quad f(U_{r+1}) \subseteq U_r.$$

By Proposition 31.14, f is an injection from U_{r+1} to U_r. Assume inductively that $U_{r+1}, \ldots, U_i$ have been defined for $i \geq 2$ and that they satisfy (1) and (2). Since

$$N_i = N_{i-1} \oplus U_i,$$

we have $U_i \subseteq N_i$, so $f^{i-1}(f(U_i)) = f^i(U_i) = (0)$, which implies that $f(U_i) \subseteq N_{i-1}$. Also, since $U_i \cap N_{i-1} = (0)$, by Proposition 31.14, we have $f(U_i) \cap N_{i-2} = (0)$. It follows that there is a supplement U_{i-1} of N_{i-2} in N_{i-1} that contains $f(U_i)$. We have

$$N_{i-1} = N_{i-2} \oplus U_{i-1} \quad \text{and} \quad f(U_i) \subseteq U_{i-1}.$$

The fact that f is an injection from U_i into U_{i-1} follows from Proposition 31.14. Therefore, the induction step is proven. The construction stops when $i = 1$. □

Because $N_0 = (0)$ and $N_{r+1} = E$, we see that E is the direct sum of the U_i:

$$E = U_1 \oplus \cdots \oplus U_{r+1},$$

with $f(U_i) \subseteq U_{i-1}$, and f an injection from U_i to U_{i-1}, for $i = r+1, \ldots, 2$. By a clever choice of bases in the U_i, we obtain the following nice theorem.

Theorem 31.16. *For any nilpotent linear map $f \colon E \to E$ on a finite-dimensional vector space E of dimension n over a field K, there is a basis of E such that the matrix N of f is of the form*

$$N = \begin{pmatrix} 0 & \nu_1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \nu_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & \nu_n \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix},$$

where $\nu_i = 1$ or $\nu_i = 0$.

Proof. First apply Proposition 31.15 to obtain a direct sum $E = \bigoplus_{i=1}^{r+1} U_i$. Then we define a basis of E inductively as follows. First we choose a basis

$$e_1^{r+1}, \ldots, e_{n_{r+1}}^{r+1}$$

of U_{r+1}. Next, for $i = r+1, \ldots, 2$, given the basis

$$e_1^i, \ldots, e_{n_i}^i$$

of U_i, since f is injective on U_i and $f(U_i) \subseteq U_{i-1}$, the vectors $f(e_1^i), \ldots, f(e_{n_i}^i)$ are linearly independent, so we define a basis of U_{i-1} by completing $f(e_1^i), \ldots, f(e_{n_i}^i)$ to a basis in U_{i-1}:

$$e_1^{i-1}, \ldots, e_{n_i}^{i-1}, e_{n_i+1}^{i-1}, \ldots, e_{n_{i-1}}^{i-1}$$

with

$$e_j^{i-1} = f(e_j^i), \quad j = 1 \ldots, n_i.$$

Since $U_1 = N_1 = \mathrm{Ker}\,(f)$, we have

$$f(e_j^1) = 0, \quad j = 1, \ldots, n_1.$$

These basis vectors can be arranged as the rows of the following matrix:

$$\begin{pmatrix}
e_1^{r+1} & \cdots & e_{n_{r+1}}^{r+1} & & & & & & & & & \\
\vdots & & \vdots & & & & & & & & & \\
e_1^{r} & \cdots & e_{n_{r+1}}^{r} & e_{n_{r+1}+1}^{r} & \cdots & e_{n_r}^{r} & & & & & & \\
\vdots & & \vdots & \vdots & & \vdots & & & & & & \\
e_1^{r-1} & \cdots & e_{n_{r+1}}^{r-1} & e_{n_{r+1}+1}^{r-1} & \cdots & e_{n_r}^{r-1} & e_{n_r+1}^{r-1} & \cdots & e_{n_{r-1}}^{r-1} & & & \\
\vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & & & \\
\vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & & & \\
e_1^{1} & \cdots & e_{n_{r+1}}^{1} & e_{n_{r+1}+1}^{1} & \cdots & e_{n_r}^{1} & e_{n_r+1}^{1} & \cdots & e_{n_{r-1}}^{1} & \cdots & \cdots & e_{n_1}^{1}
\end{pmatrix}$$

Finally, we define the basis $(e_1, \ldots, e_n)$ by listing each column of the above matrix from the bottom-up, starting with column one, then column two, *etc*. This means that we list the vectors e_j^i in the following order:

For $j = 1, \ldots, n_{r+1}$, list $e_j^1, \ldots, e_j^{r+1}$;

In general, for $i = r, \ldots, 1$,

  for $j = n_{i+1} + 1, \ldots, n_i$, list $e_j^1, \ldots, e_j^i$.

Then because $f(e_j^1) = 0$ and $e_j^{i-1} = f(e_j^i)$ for $i \geq 2$, either

$$f(e_i) = 0 \quad \text{or} \quad f(e_i) = e_{i-1},$$

which proves the theorem. □

As an application of Theorem 31.16, we obtain the *Jordan form* of a linear map.

Definition 31.7. A *Jordan block* is an $r \times r$ matrix $J_r(\lambda)$, of the form

$$J_r(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & 1 \\ 0 & 0 & 0 & \cdots & \lambda \end{pmatrix},$$

where $\lambda \in K$, with $J_1(\lambda) = (\lambda)$ if $r = 1$. A *Jordan matrix*, J, is an $n \times n$ block diagonal matrix of the form

$$J = \begin{pmatrix} J_{r_1}(\lambda_1) & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & J_{r_m}(\lambda_m) \end{pmatrix},$$

where each $J_{r_k}(\lambda_k)$ is a Jordan block associated with some $\lambda_k \in K$, and with $r_1 + \cdots + r_m = n$.

To simplify notation, we often write $J(\lambda)$ for $J_r(\lambda)$. Here is an example of a Jordan matrix with four blocks:

$$J = \begin{pmatrix} \lambda & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \lambda & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \lambda & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \mu & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mu \end{pmatrix}.$$

Theorem 31.17. *(Jordan form) Let E be a vector space of dimension n over a field K and let $f \colon E \to E$ be a linear map. The following properties are equivalent:*

(1) The eigenvalues of f all belong to K (i.e. the roots of the characteristic polynomial χ_f all belong to K).

(2) There is a basis of E in which the matrix of f is a Jordan matrix.

Proof. Assume (1). First we apply Theorem 31.11, and we get a direct sum $E = \bigoplus_{j=1}^k W_k$, such that the restriction of $g_i = f - \lambda_j\mathrm{id}$ to W_i is nilpotent. By Theorem 31.16, there is a basis of W_i such that the matrix of the restriction of g_i is of the form

$$G_i = \begin{pmatrix} 0 & \nu_1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \nu_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & \nu_{n_i} \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix},$$

where $\nu_i = 1$ or $\nu_i = 0$. Furthermore, over any basis, $\lambda_i\mathrm{id}$ is represented by the diagonal matrix D_i with λ_i on the diagonal. Then it is clear that we can split $D_i + G_i$ into Jordan blocks by forming a Jordan block for every uninterrupted chain of 1s. By putting the bases of the W_i together, we obtain a matrix in Jordan form for f.

Now assume (2). If f can be represented by a Jordan matrix, it is obvious that the diagonal entries are the eigenvalues of f, so they all belong to K. □

Observe that Theorem 31.17 applies if $K = \mathbb{C}$. It turns out that there are uniqueness properties of the Jordan blocks. There are also other fundamental normal forms for linear maps, such as the rational canonical form, but to prove these results, it is better to develop more powerful machinery about finitely generated modules over a PID. To accomplish this most effectively, we need some basic knowledge about tensor products.

If a complex $n \times n$ matrix A is expressed in terms of its Jordan decomposition as $A = D + N$, since D and N commute, by Proposition 9.21, the exponential of A is given by

$$e^A = e^D e^N,$$

and since N is an $n \times n$ nilpotent matrix, $N^{n-1} = 0$, so we obtain

$$e^A = e^D \left(I + \frac{N}{1!} + \frac{N^2}{2!} + \cdots + \frac{N^{n-1}}{(n-1)!} \right).$$

In particular, the above applies if A is a Jordan matrix. This fact can be used to solve (at least in theory) systems of first-order linear differential equations. Such systems are of the form

$$\frac{dX}{dt} = AX, \tag{$*$}$$

where A is an $n \times n$ matrix and X is an n-dimensional vector of functions of the parameter t.

It can be shown that the columns of the matrix e^{tA} form a basis of the vector space of solutions of the system of linear differential equations $(*)$; see Artin [7] (Chapter 4). Furthermore, for any matrix B and any invertible matrix P, if $A = PBP^{-1}$, then the system $(*)$ is equivalent to

$$P^{-1}\frac{dX}{dt} = BP^{-1}X,$$

so if we make the change of variable $Y = P^{-1}X$, we obtain the system

$$\frac{dY}{dt} = BY. \tag{$**$}$$

Consequently, if B is such that the exponential e^{tB} can be easily computed, we obtain an explicit solution Y of $(**)$, and $X = PY$ is an explicit solution of $(*)$. This is the case when B is a Jordan form of A. In this case, it suffices to consider the Jordan blocks of B. Then we have

$$J_r(\lambda) = \lambda I_r + \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix} = \lambda I_r + N,$$

and the powers N^k are easily computed.

For example, if

$$B = \begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 3 \end{pmatrix} = 3I_3 + \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

we obtain

$$tB = t\begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 3 \end{pmatrix} = 3tI_3 + \begin{pmatrix} 0 & t & 0 \\ 0 & 0 & t \\ 0 & 0 & 0 \end{pmatrix}$$

and so

$$e^{tB} = \begin{pmatrix} e^{3t} & 0 & 0 \\ 0 & e^{3t} & 0 \\ 0 & 0 & e^{3t} \end{pmatrix} \begin{pmatrix} 1 & t & (1/2)t^2 \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} e^{3t} & te^{3t} & (1/2)t^2e^{3t} \\ 0 & e^{3t} & te^{3t} \\ 0 & 0 & e^{3t} \end{pmatrix}.$$

The columns of e^{tB} form a basis of the space of solutions of the system of linear differential equations

$$\begin{aligned} \frac{dY_1}{dt} &= 3Y_1 + Y_2 \\ \frac{dY_2}{dt} &= 3Y_2 + Y_3 \\ \frac{dY_3}{dt} &= 3Y_3, \end{aligned}$$

in matrix form,

$$\begin{pmatrix} \frac{dY_1}{dt} \\ \frac{dY_2}{dt} \\ \frac{dY_3}{dt} \end{pmatrix} = \begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 3 \end{pmatrix} \begin{pmatrix} Y_1 \\ Y_2 \\ Y_3 \end{pmatrix}.$$

Explicitly, the general solution of the above system is

$$\begin{pmatrix} Y_1 \\ Y_2 \\ Y_3 \end{pmatrix} = c_1 \begin{pmatrix} e^{3t} \\ 0 \\ 0 \end{pmatrix} + c_2 \begin{pmatrix} te^{3t} \\ e^{3t} \\ 0 \end{pmatrix} + c_3 \begin{pmatrix} (1/2)t^2e^{3t} \\ te^{3t} \\ e^{3t} \end{pmatrix},$$

with $c_1, c_2, c_3 \in \mathbb{R}$. Solving systems of first-order linear differential equations is discussed in Artin [7] and more extensively in Hirsh and Smale [92].

31.7 Summary

The main concepts and results of this chapter are listed below:

- Ideals, principal ideals, greatest common divisors.
- Monic polynomial, irreducible polynomial, relatively prime polynomials.
- Annihilator of a linear map.
- Minimal polynomial of a linear map.

- Invariant subspace.
- f-conductor of u into W; conductor of u into W.
- Diagonalizable linear maps.
- Commuting families of linear maps.
- Primary decomposition.
- Generalized eigenvectors.
- Nilpotent linear map.
- Normal form of a nilpotent linear map.
- Jordan decomposition.
- Jordan block.
- Jordan matrix.
- Jordan normal form.
- Systems of first-order linear differential equations.

31.8 Problems

Problem 31.1. Given a linear map $f\colon E \to E$, prove that the set $\mathrm{Ann}(f)$ of polynomials that annihilate f is an ideal.

Problem 31.2. Provide the details of Proposition 31.3.

Problem 31.3. Prove that the f-conductor $S_f(u, W)$ is an ideal in $K[X]$ (Proposition 31.4).

Problem 31.4. Prove that the polynomials $g_1, \ldots, g_k$ used in the proof of Theorem 31.10 are relatively prime.

Problem 31.5. Find the minimal polynomial of the matrix

$$A = \begin{pmatrix} 6 & -3 & -2 \\ 4 & -1 & -2 \\ 10 & -5 & -3 \end{pmatrix}.$$

Problem 31.6. Find the Jordan decomposition of the matrix

$$A = \begin{pmatrix} 3 & 1 & -1 \\ 2 & 2 & -1 \\ 2 & 2 & 0 \end{pmatrix}.$$

Problem 31.7. Let $f\colon E \to E$ be a linear map on a finite-dimensional vector space. Prove that if f has rank 1, then either f is diagonalizable or f is nilpotent but not both.

Problem 31.8. Find the Jordan form of the matrix

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Problem 31.9. Let N be a 3×3 nilpotent matrix over $\mathbb{C}$. Prove that the matrix $A = I + (1/2)N - (1/8)N^2$ satisfies the equation

$$A^2 = I + N.$$

In other words, A is a square root of $I + N$.

Generalize the above fact to any $n \times n$ nilpotent matrix N over $\mathbb{C}$ using the binomial series for $(1 + t)^{1/2}$.

Problem 31.10. Let K be an algebraically closed field (for example, $K = \mathbb{C}$). Prove that every 4×4 matrix is similar to a Jordan matrix of the following form:

$$\begin{pmatrix} \lambda_1 & 0 & 0 & 0 \\ 0 & \lambda_2 & 0 & 0 \\ 0 & 0 & \lambda_3 & 0 \\ 0 & 0 & 0 & \lambda_4 \end{pmatrix}, \quad \begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \lambda_3 & 0 \\ 0 & 0 & 0 & \lambda_4 \end{pmatrix}, \quad \begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 1 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & \lambda_4 \end{pmatrix},$$

$$\begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \mu & 1 \\ 0 & 0 & 0 & \mu \end{pmatrix}, \quad \begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 1 & 0 \\ 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & \lambda \end{pmatrix}.$$

Problem 31.11. In this problem the field K is of characteristic 0. Consider an $(r \times r)$ Jordan block

$$J_r(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & 1 \\ 0 & 0 & 0 & \cdots & \lambda \end{pmatrix}.$$

Prove that for any polynomial $f(X)$, we have

$$f(J_r(\lambda)) = \begin{pmatrix} f(\lambda) & f_1(\lambda) & f_2(\lambda) & \cdots & f_{r-1}(\lambda) \\ 0 & f(\lambda) & f_1(\lambda) & \cdots & f_{r-2}(\lambda) \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & f_1(\lambda) \\ 0 & 0 & 0 & \cdots & f(\lambda) \end{pmatrix},$$

where

$$f_k(X) = \frac{f^{(k)}(X)}{k!},$$

and $f^{(k)}(X)$ is the kth derivative of $f(X)$.

Chapter 32

UFD's, Noetherian Rings, Hilbert's Basis Theorem

32.1 Unique Factorization Domains (Factorial Rings)

We saw in Section 30.5 that if K is a field, then every nonnull polynomial in $K[X]$ can be factored as a product of irreducible factors, and that such a factorization is essentially unique. The same property holds for the ring $K[X_1, \ldots, X_n]$ where $n \geq 2$, but a different proof is needed.

The reason why unique factorization holds for $K[X_1, \ldots, X_n]$ is that if A is an integral domain for which unique factorization holds in some suitable sense, then the property of unique factorization lifts to the polynomial ring $A[X]$. Such rings are called factorial rings, or unique factorization domains. The first step if to define the notion of irreducible element in an integral domain, and then to define a factorial ring. If will turn out that in a factorial ring, any nonnull element a is irreducible (or prime) iff the principal ideal (a) is a prime ideal.

Recall that given a ring A, a *unit* is any invertible element (w.r.t. multiplication). The set of units of A is denoted by A^*. It is a multiplicative subgroup of A, with identity 1. Also, given $a, b \in A$, recall that a *divides* b if $b = ac$ for some $c \in A$; equivalently, a divides b iff $(b) \subseteq (a)$. Any nonzero $a \in A$ is divisible by any unit u, since $a = u(u^{-1}a)$. The relation "a divides b," often denoted by $a \mid b$, is reflexive and transitive, and thus, a preorder on $A - \{0\}$.

Definition 32.1. Let A be an integral domain. Some element $a \in A$ is *irreducible* if $a \neq 0$, $a \notin A^*$ (a is not a unit), and whenever $a = bc$, then either b or c is a unit (where $b, c \in A$). Equivalently, $a \in A$ is *reducible* if $a = 0$, or $a \in A^*$ (a is a unit), or $a = bc$ where $b, c \notin A^*$ (a, b are both noninvertible) and $b, c \neq 0$.

Observe that if $a \in A$ is irreducible and $u \in A$ is a unit, then ua is also irreducible. Generally, if $a \in A$, $a \neq 0$, and u is a unit, then a and ua are said to be *associated*. This is the equivalence relation on nonnull elements of A induced by the divisibility preorder.

The following simple proposition gives a sufficient condition for an element $a \in A$ to be irreducible.

Proposition 32.1. *Let A be an integral domain. For any $a \in A$ with $a \neq 0$, if the principal ideal (a) is a prime ideal, then a is irreducible.*

Proof. If (a) is prime, then $(a) \neq A$ and a is not a unit. Assume that $a = bc$. Then, $bc \in (a)$, and since (a) is prime, either $b \in (a)$ or $c \in (a)$. Consider the case where $b \in (a)$, the other case being similar. Then, $b = ax$ for some $x \in A$. As a consequence,

$$a = bc = axc,$$

and since A is an integral domain and $a \neq 0$, we get

$$1 = xc,$$

which proves that $c = x^{-1}$ is a unit. □

It should be noted that the converse of Proposition 32.1 is generally false. However, it holds for factorial rings, defined next.

Definition 32.2. A *factorial ring* or *unique factorization domain (UFD)* (or *unique factorization ring*) is an integral domain A such that the following two properties hold:

(1) For every nonnull $a \in A$, if $a \notin A^*$ (a is not a unit), then a can be factored as a product

$$a = a_1 \cdots a_m$$

where each $a_i \in A$ is irreducible ($m \geq 1$).

(2) For every nonnull $a \in A$, if $a \notin A^*$ (a is not a unit) and if

$$a = a_1 \cdots a_m = b_1 \cdots b_n$$

where $a_i \in A$ and $b_j \in A$ are irreducible, then $m = n$ and there is a permutation σ of $\{1, \ldots, m\}$ and some units $u_1, \ldots, u_m \in A^*$ such that $a_i = u_i b_{\sigma(i)}$ for all i, $1 \leq i \leq m$.

Example 32.1. The ring $\mathbb{Z}$ of integers if a typical example of a UFD. Given a field K, the polynomial ring $K[X]$ is a UFD. More generally, we will show later that every PID is a UFD (see Theorem 32.12). Thus, in particular, $\mathbb{Z}[X]$ is a UFD. However, we leave as an exercise to prove that the ideal $(2X, X^2)$ generated by $2X$ and X^2 is not principal, and thus, $\mathbb{Z}[X]$ is not a PID.

First, we prove that condition (2) in Definition 32.2 is equivalent to the usual "Euclidean" condition.

There are integral domains that are not UFD's. For example, the subring $\mathbb{Z}[\sqrt{-5}]$ of $\mathbb{C}$ consisting of the complex numbers of the form $a + bi\sqrt{5}$ where $a, b \in \mathbb{Z}$ is not a UFD. Indeed, we have

$$9 = 3 \cdot 3 = (2 + i\sqrt{5})(2 - i\sqrt{5}),$$

and it can be shown that 3, $2 + i\sqrt{5}$, and $2 - i\sqrt{5}$ are irreducible, and that the units are ± 1. The uniqueness condition (2) fails and $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Remark: For $d \in \mathbb{Z}$ with $d < 0$, it is known that the ring of integers of $\mathbb{Q}(\sqrt{d})$ is a UFD iff d is one of the nine primes, $d = -1, -2, -3, -7, -11, -19, -43, -67$ and -163. This is a hard theorem that was conjectured by Gauss but not proved until 1966, independently by Stark and Baker. Heegner had published a proof of this result in 1952 but there was some doubt about its validity. After finding his proof, Stark reexamined Heegner's proof and concluded that it was essentially correct after all. In sharp contrast, when d is a positive integer, the problem of determining which of the rings of integers of $\mathbb{Q}(\sqrt{d})$ are UFD's, is still open. It can also be shown that if $d < 0$, then the ring $\mathbb{Z}[\sqrt{d}]$ is a UFD iff $d = -1$ or $d = -2$. If $d \equiv 1 \pmod 4$, then $\mathbb{Z}[\sqrt{d}]$ is never a UFD. For more details about these remarkable results, see Stark [162] (Chapter 8).

Proposition 32.2. *Let A be an integral domain satisfying condition* (1) *in Definition 32.2. Then, condition* (2) *in Definition 32.2 is equivalent to the following condition:*

(2′) If $a \in A$ is irreducible and a divides the product bc, where $b, c \in A$ and $b, c \neq 0$, then either a divides b or a divides c.

Proof. First, assume that (2) holds. Let $bc = ad$, where $d \in A$, $d \neq 0$. If b is a unit, then

$$c = adb^{-1},$$

and c is divisible by a. A similar argument applies to c. Thus, we may assume that b and c are not units. In view of (1), we can write

$$b = p_1 \cdots p_m \quad \text{and} \quad c = p_{m+1} \cdots q_{m+n},$$

where $p_i \in A$ is irreducible. Since $bc = ad$, a is irreducible, and b, c are not units, d cannot be a unit. In view of (1), we can write

$$d = q_1 \cdots q_r,$$

where $q_i \in A$ is irreducible. Thus,

$$p_1 \cdots p_m p_{m+1} \cdots p_{m+n} = a q_1 \cdots q_r,$$

where all the factors involved are irreducible. By (2), we must have

$$a = u_{i_0} p_{i_0}$$

for some unit $u_{i_0} \in A$ and some index i_0, $1 \leq i_0 \leq m+n$. As a consequence, if $1 \ \leq i_0 \leq m$, then a divides b, and if $m+1 \leq i_0 \leq m+n$, then a divides c. This proves that $(2')$ holds.

Let us now assume that $(2')$ holds. Assume that

$$a = a_1 \cdots a_m = b_1 \cdots b_n,$$

where $a_i \in A$ and $b_j \in A$ are irreducible. Without loss of generality, we may assume that $m \leq n$. We proceed by induction on m. If $m = 1$,

$$a_1 = b_1 \cdots b_n,$$

and since a_1 is irreducible, $u = b_1 \cdots b_{i-1} b_{i+1} b_n$ must be a unit for some i, $1 \leq i \leq n$. Thus, (2) holds with $n = 1$ and $a_1 = b_i u$. Assume that $m > 1$ and that the induction hypothesis holds for $m - 1$. Since

$$a_1 a_2 \cdots a_m = b_1 \cdots b_n,$$

a_1 divides $b_1 \cdots b_n$, and in view of $(2')$, a_1 divides some b_j. Since a_1 and b_j are irreducible, we must have $b_j = u_j a_1$, where $u_j \in A$ is a unit. Since A is an integral domain,

$$a_1 a_2 \cdots a_m = b_1 \cdots b_{j-1} u_j a_1 b_{j+1} \cdots b_n$$

implies that

$$a_2 \cdots a_m = (u_j b_1) \cdots b_{j-1} b_{j+1} \cdots b_n,$$

and by the induction hypothesis, $m - 1 = n - 1$ and $a_i = v_i b_{\tau(i)}$ for some units $v_i \in A$ and some bijection τ between $\{2, \ldots, m\}$ and $\{1, \ldots, j-1, j+1, \ldots, m\}$. However, the bijection τ extends to a permutation σ of $\{1, \ldots, m\}$ by letting $\sigma(1) = j$, and the result holds by letting $v_1 = u_j^{-1}$. □

As a corollary of Proposition 32.2. we get the converse of Proposition 32.1.

Proposition 32.3. *Let A be a factorial ring. For any $a \in A$ with $a \neq 0$, the principal ideal (a) is a prime ideal iff a is irreducible.*

Proof. In view of Proposition 32.1, we just have to prove that if $a \in A$ is irreducible, then the principal ideal (a) is a prime ideal. Indeed, if $bc \in (a)$, then a divides bc, and by Proposition 32.2, property $(2')$ implies that either a divides b or a divides c, that is, either $b \in (a)$ or $c \in (a)$, which means that (a) is prime. □

Because Proposition 32.3 holds, in a UFD, an irreducible element is often called a *prime*.

In a UFD A, every nonzero element $a \in A$ that is not a unit can be expressed as a product $a = a_1 \cdots a_n$ of irreducible elements a_i, and by property (2), the number n of factors only depends on a, that is, it is the same for all factorizations into irreducible factors. We agree that this number is 0 for a unit.

Remark: If A is a UFD, we can state the factorization properties so that they also applies to units:

(1) For every nonnull $a \in A$, a can be factored as a product

$$a = ua_1 \cdots a_m$$

where $u \in A^*$ (u is a unit) and each $a_i \in A$ is irreducible ($m \geq 0$).

(2) For every nonnull $a \in A$, if

$$a = ua_1 \cdots a_m = vb_1 \cdots b_n$$

where $u, v \in A^*$ (u, v are units) and $a_i \in A$ and $b_j \in A$ are irreducible, then $m = n$, and if $m = n = 0$ then $u = v$, else if $m \geq 1$, then there is a permutation σ of $\{1, \ldots, m\}$ and some units $u_1, \ldots, u_m \in A^*$ such that $a_i = u_i b_{\sigma(i)}$ for all i, $1 \leq i \leq m$.

We are now ready to prove that if A is a UFD, then the polynomial ring $A[X]$ is also a UFD.

First, observe that the units of $A[X]$ are just the units of A. The fact that nonnull and nonunit polynomials in $A[X]$ factor as products of irreducible polynomials is easier to prove than uniqueness. We will show in the proof of Theorem 32.10 that we can proceed by induction on the pairs (m, n) where m is the degree of $f(X)$ and n is either 0 if the coefficient f_m of X^m in $f(X)$ is a unit of n is f_m is the product of n irreducible elements.

For the uniqueness of the factorization, by Proposition 32.2, it is enough to prove that condition ($2'$) holds. This is a little more tricky. There are several proofs, but they all involve a pretty Lemma due to Gauss.

First, note the following trivial fact. Given a ring A, for any $a \in A$, $a \neq 0$, if a divides every coefficient of some nonnull polynomial $f(X) \in A[X]$, then a divides $f(X)$. If A is an integral domain, we get the following converse.

Proposition 32.4. *Let A be an integral domain. For any $a \in A$, $a \neq 0$, if a divides a nonnull polynomial $f(X) \in A[X]$, then a divides every coefficient of $f(X)$.*

Proof. Assume that $f(X) = ag(X)$, for some $g(X) \in A[X]$. Since $a \neq 0$ and A is an integral ring, $f(X)$ and $g(X)$ have the same degree m, and since for every i ($0 \leq i \leq m$) the coefficient of X^i in $f(X)$ is equal to the coefficient of X^i in $ag(x)$, we have $f_i = ag_i$, and whenever $f_i \neq 0$, we see that a divides f_i. □

Lemma 32.5. *(Gauss's lemma) Let A be a UFD. For any $a \in A$, if a is irreducible and a divides the product $f(X)g(X)$ of two polynomials $f(X), g(X) \in A[X]$, then either a divides $f(X)$ or a divides $g(X)$.*

Proof. Let $f(X) = f_m X^m + \cdots + f_i X^i + \cdots + f_0$ and $g(X) = g_n X^n + \cdots + g_j X^j + \cdots + g_0$. Assume that a divides neither $f(X)$ nor $g(X)$. By the (easy) converse of Proposition 32.4, there is some i ($0 \leq i \leq m$) such that a does not divide f_i, and there is some j ($0 \leq j \leq n$)

such that a does not divide g_j. Pick i and j minimal such that a does not divide f_i and a does not divide g_j. The coefficient c_{i+j} of X^{i+j} in $f(X)g(X)$ is

$$c_{i+j} = f_0 g_{i+j} + f_1 g_{i+j-1} + \cdots + f_i g_j + \cdots + f_{i+j} g_0$$

(letting $f_h = 0$ if $h > m$ and $g_k = 0$ if $k > n$). From the choice of i and j, a cannot divide $f_i g_j$, since a being irreducible, by (2′) of Proposition 32.2, a would divide f_i or g_j. However, by the choice of i and j, a divides every other nonnull term in the sum for c_{i+j}, and since a is irreducible and divides $f(X)g(X)$, by Proposition 32.4, a divides c_{i+j}, which implies that a divides $f_i g_j$, a contradiction. Thus, either a divides $f(X)$ or a divides $g(X)$. □

As a corollary, we get the following proposition.

Proposition 32.6. *Let A be a UFD. For any $a \in A$, $a \neq 0$, if a divides the product $f(X)g(X)$ of two polynomials $f(X), g(X) \in A[X]$ and $f(X)$ is irreducible and of degree at least 1, then a divides $g(X)$.*

Proof. The Proposition is trivial is a is a unit. Otherwise, $a = a_1 \cdots a_m$ where $a_i \in A$ is irreducible. Using induction and applying Lemma 32.5, we conclude that a divides $g(X)$. □

We now show that Lemma 32.5 also applies to the case where a is an irreducible polynomial. This requires a little excursion involving the fraction field F of A.

Remark: If A is a UFD, it is possible to prove the uniqueness condition (2) for $A[X]$ directly without using the fraction field of A, see Malliavin [118], Chapter 3.

Given an integral domain A, we can construct a field F such that every element of F is of the form a/b, where $a, b \in A$, $b \neq 0$, using essentially the method for constructing the field $\mathbb{Q}$ of rational numbers from the ring $\mathbb{Z}$ of integers.

Proposition 32.7. *Let A be an integral domain.*

(1) There is a field F and an injective ring homomorphism $i\colon A \to F$ such that every element of F is of the form $i(a)i(b)^{-1}$, where $a, b \in A$, $b \neq 0$.

(2) For every field K and every injective ring homomorphism $h\colon A \to K$, there is a (unique) field homomorphism $\widehat{h}\colon F \to K$ such that

$$\widehat{h}(i(a)i(b)^{-1}) = h(a)h(b)^{-1}$$

for all $a, b \in A$, $b \neq 0$.

(3) The field F in (1) is unique up to isomorphism.

Proof. (1) Consider the binary relation $\simeq$ on $A \times (A - \{0\})$ defined as follows:

$$(a, b) \simeq (a', b') \quad \text{iff} \quad ab' = a'b.$$

It is easily seen that $\simeq$ is an equivalence relation. Note that the fact that A is an integral domain is used to prove transitivity. The equivalence class of (a, b) is denoted by a/b. Clearly, $(0, b) \simeq (0, 1)$ for all $b \in A$, and we denote the class of $(0, 1)$ also by 0. The equivalence class $a/1$ of $(a, 1)$ is also denoted by a. We define addition and multiplication on $A \times (A - \{0\})$ as follows:

$$\begin{aligned}(a, b) + (a', b') &= (ab' + a'b, bb'),\\ (a, b) \cdot (a', b') &= (aa', bb').\end{aligned}$$

It is easily verified that $\simeq$ is congruential w.r.t. $+$ and $\cdot$, which means that $+$ and $\cdot$ are well-defined on equivalence classes modulo $\simeq$. When $a, b \neq 0$, the inverse of a/b is b/a, and it is easily verified that F is a field. The map $i \colon A \to F$ defined such that $i(a) = a/1$ is an injection of A into F and clearly

$$\frac{a}{b} = i(a)i(b)^{-1}.$$

(2) Given an injective ring homomorphism $h \colon A \to K$ into a field K,

$$\frac{a}{b} = \frac{a'}{b'} \quad \text{iff} \quad ab' = a'b,$$

which implies that

$$h(a)h(b') = h(a')h(b),$$

and since h is injective and $b, b' \neq 0$, we get

$$h(a)h(b)^{-1} = h(a')h(b')^{-1}.$$

Thus, there is a map $\widehat{h} \colon F \to K$ such that

$$\widehat{h}(a/b) = \widehat{h}(i(a)i(b)^{-1}) = h(a)h(b)^{-1}$$

for all $a, b \in A$, $b \neq 0$, and it is easily checked that $\widehat{h}$ is a field homomorphism. The map $\widehat{h}$ is clearly unique.

(3) The uniqueness of F up to isomorphism follows from (2), and is left as an exercise. □

The field F given by Proposition 32.7 is called the *fraction field of* A, and it is denoted by $\mathrm{Frac}(A)$.

In particular, given an integral domain A, since $A[X_1, \ldots, X_n]$ is also an integral domain, we can form the fraction field of the polynomial ring $A[X_1, \ldots, X_n]$, denoted by $F(X_1, \ldots, X_n)$, where $F = \mathrm{Frac}(A)$ is the fraction field of A. It is also called the field of *rational functions* over F, although the terminology is a bit misleading, since elements of $F(X_1, \ldots, X_n)$ only define functions when the dominator is nonnull.

We now have the following crucial lemma which shows that if a polynomial $f(X)$ is reducible over $F[X]$ where F is the fraction field of A, then $f(X)$ is already reducible over $A[X]$.

Lemma 32.8. *Let A be a UFD and let F be the fraction field of A. For any nonnull polynomial $f(X) \in A[X]$ of degree m, if $f(X)$ is not the product of two polynomials of degree strictly smaller than m, then $f(X)$ is irreducible in $F[X]$.*

Proof. Assume that $f(X)$ is reducible in $F[X]$ and that $f(X)$ is neither null nor a unit. Then,

$$f(X) = G(X)H(X),$$

where $G(X), H(X) \in F[X]$ are polynomials of degree $p, q \geq 1$. Let a be the product of the denominators of the coefficients of $G(X)$, and b the product of the denominators of the coefficients of $H(X)$. Then, $a, b \neq 0$, $g_1(X) = aG(X) \in A[X]$ has degree $p \geq 1$, $h_1(X) = bH(X) \in A[X]$ has degree $q \geq 1$, and

$$abf(X) = g_1(X)h_1(X).$$

Let $c = ab$. If c is a unit, then $f(X)$ is also reducible in $A[X]$. Otherwise, $c = c_1 \cdots c_n$, where $c_i \in A$ is irreducible. We now use induction on n to prove that

$$f(X) = g(X)h(X),$$

for some polynomials $g(X) \in A[X]$ of degree $p \geq 1$ and $h(X) \in A[X]$ of degree $q \geq 1$.

If $n = 1$, since $c = c_1$ is irreducible, by Lemma 32.5, either c divides $g_1(X)$ or c divides $h_1(X)$. Say that c divides $g_1(X)$, the other case being similar. Then, $g_1(X) = cg(X)$ for some $g(X) \in A[X]$ of degree $p \geq 1$, and since $A[X]$ is an integral ring, we get

$$f(X) = g(X)h_1(X),$$

showing that $f(X)$ is reducible in $A[X]$. If $n > 1$, since

$$c_1 \cdots c_n f(X) = g_1(X)h_1(X),$$

c_1 divides $g_1(X)h_1(X)$, and as above, either c_1 divides $g_1(X)$ or c divides $h_1(X)$. In either case, we get

$$c_2 \cdots c_n f(X) = g_2(X)h_2(X)$$

for some polynomials $g_2(X) \in A[X]$ of degree $p \geq 1$ and $h_2(X) \in A[X]$ of degree $q \geq 1$. By the induction hypothesis, we get

$$f(X) = g(X)h(X),$$

for some polynomials $g(X) \in A[X]$ of degree $p \geq 1$ and $h(X) \in A[X]$ of degree $q \geq 1$, showing that $f(X)$ is reducible in $A[X]$. □

Finally, we can prove that (2′) holds.

Lemma 32.9. *Let A be a UFD. Given any three nonnull polynomials $f(X), g(X), h(X) \in A[X]$, if $f(X)$ is irreducible and $f(X)$ divides the product $g(X)h(X)$, then either $f(X)$ divides $g(X)$ or $f(X)$ divides $h(X)$.*

Proof. If $f(X)$ has degree 0, then the result follows from Lemma 32.5. Thus, we may assume that the degree of $f(X)$ is $m \geq 1$. Let F be the fraction field of A. By Lemma 32.8, $f(X)$ is also irreducible in $F[X]$. Since $F[X]$ is a UFD (by Theorem 30.17), either $f(X)$ divides $g(X)$ or $f(X)$ divides $h(X)$, in $F[X]$. Assume that $f(X)$ divides $g(X)$, the other case being similar. Then,

$$g(X) = f(X)G(X),$$

for some $G(X) \in F[X]$. If a is the product the denominators of the coefficients of G, we have

$$ag(X) = q_1(X)f(X),$$

where $q_1(X) = aG(X) \in A[X]$. If a is a unit, we see that $f(X)$ divides $g(X)$. Otherwise, $a = a_1 \cdots a_n$, where $a_i \in A$ is irreducible. We prove by induction on n that

$$g(X) = q(X)f(X)$$

for some $q(X) \in A[X]$.

If $n = 1$, since $f(X)$ is irreducible and of degree $m \geq 1$ and

$$a_1 g(X) = q_1(X)f(X),$$

by Lemma 32.5, a_1 divides $q_1(X)$. Thus, $q_1(X) = a_1 q(X)$ where $q(X) \in A[X]$. Since $A[X]$ is an integral domain, we get

$$g(X) = q(X)f(X),$$

and $f(X)$ divides $g(X)$. If $n > 1$, from

$$a_1 \cdots a_n g(X) = q_1(X)f(X),$$

we note that a_1 divides $q_1(X)f(X)$, and as in the previous case, a_1 divides $q_1(X)$. Thus, $q_1(X) = a_1 q_2(X)$ where $q_2(X) \in A[X]$, and we get

$$a_2 \cdots a_n g(X) = q_2(X)f(X).$$

By the induction hypothesis, we get

$$g(X) = q(X)f(X)$$

for some $q(X) \in A[X]$, and $f(X)$ divides $g(X)$. □

We finally obtain the fact that $A[X]$ is a UFD when A is.

Theorem 32.10. *If A is a UFD then the polynomial ring $A[X]$ is also a UFD.*

Proof. As we said earlier, the factorization property (1) is easier to prove than uniqueness. Assume that $f(X)$ has degree m and let f_m be the coefficient of X^m in $f(X)$. Either f_m is a unit or it is the product of $n \geq 1$ irreducible elements. If f_m is a unit we set $n = 0$. We proceed by induction on the pair (m, n), using the well-founded ordering on pairs, i.e.,

$$(m, n) \leq (m', n')$$

iff either $m < m'$, or $m = m'$ and $n < n'$. If $f(X)$ is a nonnull polynomial of degree 0 which is not a unit, then $f(X) \in A$, and $f(X) = f_m = a_1 \cdots a_n$ for some irreducible $a_i \in A$, since A is a UFD. This proves the base case.

If $f(X)$ has degree $m > 0$ and $f(X)$ is reducible, then

$$f(X) = g(X)h(X),$$

where $g(X)$ and $h(X)$ have degree $p, q \leq m$ and are not units. There are two cases.

(1) f_m is a unit (so $n = 0$).

If so, since $f_m = g_p h_q$ (where g_p is the coefficient of X^p in $g(X)$ and h_q is the coefficient of X^q in $h(X)$), then g_p and h_q are both units. We claim that $p, q \geq 1$. Otherwise, $p = 0$ or $q = 0$, but then either $g(X) = g_0$ is a unit or $h(X) = h_0$ is a unit, a contradiction.

Now, since $m = p + q$ and $p, q \geq 1$, we have $p, q < m$ so $(p, 0) < (m, 0)$ and $(q, 0) < (m, 0)$, and by the induction hypothesis, both $g(X)$ and $h(X)$ can be written as products of irreducible factors, thus so can $f(X)$.

(2) f_m is not a unit, say $f_m = a_1 \cdots a_n$ where $a_1, \ldots, a_n$ are irreducible and $n \geq 1$.

(a) If $p, q < m$, then $(p, n_1) < (m, n)$ and $(q, n_2) < (m, n)$ where n_1 is the number of irreducible factors of g_p or $n_1 = 0$ if g_p is irreducible, and similarly n_2 is the number of irreducible factors of h_p or $n_2 = 0$ if h_p is irreducible (note that $n_1, n_2 \leq n$ and it is possible that $n_1 = n$ if h_q is irreducible or $n_2 = n$ if g_p is irreducible). By the induction hypothesis, $g(X)$ and $h(X)$ can be written as products of irreducible polynomials, thus so can $f(X)$.

(b) If $p = 0$ and $q = m$, then $g(X) = g_p$ and by hypothesis g_p is not a unit. Since $f_m = a_1 \cdots a_n = g_p h_q$ and g_p is not a unit, either h_q is not a unit in which case, by the uniqueness of the number of irreducible elements in the decomposition of f_m (since A is a UFD), h_q is the product of $n_2 < n$ irreducible elements, or $n_2 = 0$ if h_q is irreducible. Since $n \geq 1$, this implies that $(m, n_2) < (m, n)$, and by the induction hypothesis $h(X)$ can be written as products of irreducible polynomials. Since $g_p \in A$ is not a unit, it can also be written as a product of irreducible elements, thus so can $f(X)$.

The case where $p = m$ and $q = 0$ is similar to the previous case.

Property (2′) follows by Lemma 32.9. By Proposition 32.2, $A[X]$ is a UFD. □

As a corollary of Theorem 32.10 and using induction, we note that for any field K, the polynomial ring $K[X_1, \ldots, X_n]$ is a UFD.

For the sake of completeness, we shall prove that every PID is a UFD. First, we review the notion of gcd and the characterization of gcd's in a PID.

Given an integral domain A, for any two elements $a, b \in A$, $a, b \neq 0$, we say that $d \in A$ ($d \neq 0$) is a *greatest common divisor (gcd)* of a and b if

(1) d divides both a and b.

(2) For any $h \in A$ ($h \neq 0$), if h divides both a and b, then h divides d.

We also say that a and b are *relatively prime* if 1 is a gcd of a and b.

Note that a and b are relatively prime iff every gcd of a and b is a unit. If A is a PID, then gcd's are characterized as follows.

Proposition 32.11. *Let A be a PID.*

(1) For any $a, b, d \in A$ ($a, b, d \neq 0$), d is a gcd of a and b iff

$$(d) = (a, b) = (a) + (b),$$

i.e., d generates the principal ideal generated by a and b.

(2) (Bezout identity) Two nonnull elements $a, b \in A$ are relatively prime iff there are some $x, y \in A$ such that

$$ax + by = 1.$$

Proof. (1) Recall that the ideal generated by a and b is the set

$$(a) + (b) = aA + bA = \{ax + by \mid x, y \in A\}.$$

First, assume that d is a gcd of a and b. If so, $a \in Ad$, $b \in Ad$, and thus, $(a) \subseteq (d)$ and $(b) \subseteq (d)$, so that

$$(a) + (b) \subseteq (d).$$

Since A is a PID, there is some $t \in A$, $t \neq 0$, such that

$$(a) + (b) = (t),$$

and thus, $(a) \subseteq (t)$ and $(b) \subseteq (t)$, which means that t divides both a and b. Since d is a gcd of a and b, t must divide d. But then,

$$(d) \subseteq (t) = (a) + (b),$$

and thus, $(d) = (a) + (b)$.

Assume now that

$$(d) = (a) + (b) = (a, b).$$

Since $(a) \subseteq (d)$ and $(b) \subseteq (d)$, d divides both a and b. Assume that t divides both a and b, so that $(a) \subseteq (t)$ and $(b) \subseteq (t)$. Then,

$$(d) = (a) + (b) \subseteq (t),$$

which means that t divides d, and d is indeed a gcd of a and b.

(2) By (1), if a and b are relatively prime, then

$$(1) = (a) + (b),$$

which yields the result. Conversely, if

$$ax + by = 1,$$

then

$$(1) = (a) + (b),$$

and 1 is a gcd of a and b. □

Given two nonnull elements $a, b \in A$, if a is an irreducible element and a does not divide b, then a and b are relatively prime. Indeed, if d is not a unit and d divides both a and b, then $a = dp$ and $b = dq$ where p must be a unit, so that

$$b = ap^{-1}q,$$

and a divides b, a contradiction.

Theorem 32.12. *Let A be ring. If A is a PID, then A is a UFD.*

Proof. First, we prove that every nonnull element that is a not a unit can be factored as a product of irreducible elements. Let $\mathcal{S}$ be the set of nontrivial principal ideals (a) such that $a \neq 0$ is not a unit and cannot be factored as a product of irreducible elements (in particular, a is not irreducible). Assume that $\mathcal{S}$ is nonempty. We claim that every ascending chain in $\mathcal{S}$ is finite. Otherwise, consider an infinite ascending chain

$$(a_1) \subset (a_2) \subset \cdots \subset (a_n) \subset \cdots .$$

It is immediately verified that

$$\bigcup_{n \geq 1} (a_n)$$

is an ideal in A. Since A is a PID,

$$\bigcup_{n \geq 1} (a_n) = (a)$$

for some $a \in A$. However, there must be some n such that $a \in (a_n)$, and thus,

$$(a_n) \subseteq (a) \subseteq (a_n),$$

and the chain stabilizes at (a_n).

As a consequence, there are maximal ideals in $\mathcal{S}$. Let (a) be a maximal ideal in $\mathcal{S}$. Then, for any ideal (d) such that

$$(a) \subset (d) \quad \text{and} \quad (a) \neq (d),$$

we must have $d \notin \mathcal{S}$, since otherwise (a) would not be a maximal ideal in $\mathcal{S}$. Observe that a is not irreducible, since $(a) \in \mathcal{S}$, and thus,

$$a = bc$$

for some $b, c \in A$, where neither b nor c is a unit. Then,

$$(a) \subseteq (b) \quad \text{and} \quad (a) \subseteq (c).$$

If $(a) = (b)$, then $b = au$ for some $u \in A$, and then

$$a = auc,$$

so that

$$1 = uc,$$

since A is an integral domain, and thus, c is a unit, a contradiction. Thus, $(a) \neq (b)$, and similarly, $(a) \neq (c)$. But then, by a previous observation $b \notin \mathcal{S}$ and $c \notin \mathcal{S}$, and since a and b are not units, both b and c factor as products of irreducible elements and so does $a = bc$, a contradiction. This implies that $\mathcal{S} = \emptyset$, so every nonnull element that is a not a unit can be factored as a product of irreducible elements

To prove the uniqueness of factorizations, we use Proposition 32.2. Assume that a is irreducible and that a divides bc. If a does not divide b, by a previous remark, a and b are relatively prime, and by Proposition 32.11, there are some $x, y \in A$ such that

$$ax + by = 1.$$

Thus,

$$acx + bcy = c,$$

and since a divides bc, we see that a must divide c, as desired. □

Thus, we get another justification of the fact that $\mathbb{Z}$ is a UFD and that if K is a field, then $K[X]$ is a UFD.

It should also be noted that in a UFD, gcd's of nonnull elements always exist. Indeed, this is trivial if a or b is a unit, and otherwise, we can write

$$a = p_1 \cdots p_m \quad \text{and} \quad b = q_1 \cdots q_n$$

where $p_i, q_j \in A$ are irreducible, and the product of the common factors of a and b is a gcd of a and b (it is 1 is there are no common factors).

We conclude this section on UFD's by proving a proposition characterizing when a UFD is a PID. The proof is nontrivial and makes use of Zorn's lemma (several times).

Proposition 32.13. *Let A be a ring that is a UFD, and not a field. Then, A is a PID iff every nonzero prime ideal is maximal.*

Proof. Assume that A is a PID that is not a field. Consider any nonzero prime ideal, (p), and pick any proper ideal $\mathfrak{A}$ in A such that

$$(p) \subseteq \mathfrak{A}.$$

Since A is a PID, the ideal $\mathfrak{A}$ is a principal ideal, so $\mathfrak{A} = (q)$, and since $\mathfrak{A}$ is a proper nonzero ideal, $q \neq 0$ and q is not a unit. Since

$$(p) \subseteq (q),$$

q divides p, and we have $p = qp_1$ for some $p_1 \in A$. Now, by Proposition 32.1, since $p \neq 0$ and (p) is a prime ideal, p is irreducible. But then, since $p = qp_1$ and p is irreducible, p_1 must be a unit (since q is not a unit), which implies that

$$(p) = (q);$$

that is, (p) is a maximal ideal.

Conversely, let us assume that every nonzero prime ideal is maximal. First, we prove that every prime ideal is principal. This is obvious for (0). If $\mathfrak{A}$ is a nonzero prime ideal, then, by hypothesis, it is maximal. Since $\mathfrak{A} \neq (0)$, there is some nonzero element $a \in \mathfrak{A}$. Since $\mathfrak{A}$ is maximal, a is not a unit, and since A is a UFD, there is a factorization $a = a_1 \cdots a_n$ of a into irreducible elements. Since $\mathfrak{A}$ is prime, we have $a_i \in \mathfrak{A}$ for some i. Now, by Proposition 32.3, since a_i is irreducible, the ideal (a_i) is prime, and so, by hypothesis, (a_i) is maximal. Since $(a_i) \subseteq \mathfrak{A}$ and (a_i) is maximal, we get $\mathfrak{A} = (a_i)$.

Next, assume that A is not a PID. Define the set, $\mathcal{F}$, by

$$\mathcal{F} = \{\mathfrak{A} \mid \mathfrak{A} \subseteq A, \quad \mathfrak{A} \text{ is not a principal ideal}\}.$$

Since A is not a PID, the set $\mathcal{F}$ is nonempty. Also, the reader will easily check that every chain in $\mathcal{F}$ is bounded in $\mathcal{F}$. Indeed, for any chain $(\mathfrak{A}_i)_{i \in I}$ of ideals in $\mathcal{F}$ it is not hard to verify that $\bigcup_{i \in I} \mathfrak{A}_i$ is an ideal which is not principal, so $\bigcup_{i \in I} \mathfrak{A}_i \in \mathcal{F}$. Then, by Zorn's lemma (Lemma B.1), the set $\mathcal{F}$ has some maximal element, $\mathfrak{A}$. Clearly, $\mathfrak{A} \neq (0)$ is a proper ideal (since $A = (1)$), and $\mathfrak{A}$ is not prime, since we just showed that prime ideals are principal. Then, by Theorem B.3, there is some maximal ideal, $\mathfrak{M}$, so that $\mathfrak{A} \subset \mathfrak{M}$. However, a maximal ideal is prime, and we have shown that a prime ideal is principal. Thus,

$$\mathfrak{A} \subseteq (p),$$

for some $p \in A$ that is not a unit. Moreover, by Proposition 32.1, the element p is irreducible. Define

$$\mathfrak{B} = \{a \in A \mid pa \in \mathfrak{A}\}.$$

Clearly, $\mathfrak{A} = p\mathfrak{B}$, $\mathfrak{B} \neq (0)$, $\mathfrak{A} \subseteq \mathfrak{B}$, and $\mathfrak{B}$ is a proper ideal. We claim that $\mathfrak{A} \neq \mathfrak{B}$. Indeed, if $\mathfrak{A} = \mathfrak{B}$ were true, then we would have $\mathfrak{A} = p\mathfrak{B} = \mathfrak{B}$, but this is impossible since p is irreducible, A is a UFD, and $\mathfrak{B} \neq (0)$ (we get $\mathfrak{B} = p^m\mathfrak{B}$ for all m, and every element of $\mathfrak{B}$ would be a multiple of p^m for arbitrarily large m, contradicting the fact that A is a UFD). Thus, we have $\mathfrak{A} \subset \mathfrak{B}$, and since $\mathfrak{A}$ is a maximal element of $\mathcal{F}$, we must have $\mathfrak{B} \notin \mathcal{F}$. However, $\mathfrak{B} \notin \mathcal{F}$ means that $\mathfrak{B}$ is a principal ideal, and thus, $\mathfrak{A} = p\mathfrak{B}$ is also a principal ideal, a contradiction. □

Observe that the above proof shows that Proposition 32.13 also holds under the assumption that every prime ideal is principal.

32.2 The Chinese Remainder Theorem

In this section, which is a bit of an interlude, we prove a basic result about quotients of commutative rings by products of ideals that are pairwise relatively prime. This result has applications in number theory and in the structure theorem for finitely generated modules over a PID, which will be presented later.

Given two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of a ring A, we define the ideal $\mathfrak{a}\mathfrak{b}$ as the set of all finite sums of the form

$$a_1b_1 + \cdots + a_kb_k, \quad a_i \in \mathfrak{a},\ b_i \in \mathfrak{b}.$$

The reader should check that $\mathfrak{a}\mathfrak{b}$ is indeed an ideal. Observe that $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}$ and $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b}$, so that

$$\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}.$$

In general equality does not hold. However if

$$\mathfrak{a} + \mathfrak{b} = A,$$

then we have

$$\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}.$$

This is because there is some $a \in \mathfrak{a}$ and some $b \in \mathfrak{b}$ such that

$$a + b = 1,$$

so for every $x \in \mathfrak{a} \cap \mathfrak{b}$, we have

$$x = xa + xb,$$

which shows that $x \in \mathfrak{a}\mathfrak{b}$. Ideals $\mathfrak{a}$ and $\mathfrak{b}$ of A that satisfy the condition $\mathfrak{a} + \mathfrak{b} = A$ are sometimes said to be *comaximal*.

We define the homomorphism $\varphi\colon A \to A/\mathfrak{a} \times A/\mathfrak{b}$ by

$$\varphi(x) = (\overline{x}_{\mathfrak{a}}, \overline{x}_{\mathfrak{b}}),$$

where $\overline{x}_{\mathfrak{a}}$ is the equivalence class of x modulo $\mathfrak{a}$ (resp. $\overline{x}_{\mathfrak{b}}$ is the equivalence class of x modulo $\mathfrak{b}$). Recall that the ideal $\mathfrak{a}$ defines the equivalence relation $\equiv_{\mathfrak{a}}$ on A given by

$$x \equiv_{\mathfrak{a}} y \quad \text{iff} \quad x - y \in \mathfrak{a},$$

and that $A/\mathfrak{a}$ is the quotient ring of equivalence classes $\overline{x}_{\mathfrak{a}}$, where $x \in A$, and similarly for $A/\mathfrak{b}$. Sometimes, we also write $x \equiv y \pmod{\mathfrak{a}}$ for $x \equiv_{\mathfrak{a}} y$.

Clearly, the kernel of the homomorphism φ is $\mathfrak{a} \cap \mathfrak{b}$. If we assume that $\mathfrak{a} + \mathfrak{b} = A$, then $\mathrm{Ker}\,(\varphi) = \mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$, and because φ has a constant value on the equivalence classes modulo $\mathfrak{a}\mathfrak{b}$, the map φ induces a quotient homomorphism

$$\theta\colon A/\mathfrak{a}\mathfrak{b} \to A/\mathfrak{a} \times A/\mathfrak{b}.$$

Because $\mathrm{Ker}\,(\varphi) = \mathfrak{a}\mathfrak{b}$, the homomorphism θ is injective. The Chinese Remainder Theorem says that θ is an isomorphism.

Theorem 32.14. *Given a commutative ring A, let $\mathfrak{a}$ and $\mathfrak{b}$ be any two ideals of A such that $\mathfrak{a} + \mathfrak{b} = A$. Then, the homomorphism $\theta\colon A/\mathfrak{a}\mathfrak{b} \to A/\mathfrak{a} \times A/\mathfrak{b}$ is an isomorphism.*

Proof. We already showed that θ is injective, so we need to prove that θ is surjective. We need to prove that for any $y, z \in A$, there is some $x \in A$ such that

$$\begin{aligned} x &\equiv y \pmod{\mathfrak{a}} \\ x &\equiv z \pmod{\mathfrak{b}}. \end{aligned}$$

Since $\mathfrak{a} + \mathfrak{b} = A$, there exist some $a \in \mathfrak{a}$ and some $b \in \mathfrak{b}$ such that

$$a + b = 1.$$

If we let

$$x = az + by,$$

then we have

$$x \equiv_{\mathfrak{a}} by \equiv_{\mathfrak{a}} (1 - a)y \equiv_{\mathfrak{a}} y - ay \equiv_{\mathfrak{a}} y,$$

and similarly

$$x \equiv_{\mathfrak{b}} az \equiv_{\mathfrak{b}} (1 - b)z \equiv_{\mathfrak{b}} z - bz \equiv_{\mathfrak{b}} z,$$

which shows that $x = az + by$ works. □

Theorem 32.14 can be generalized to any (finite) number of ideals.

Theorem 32.15. *(Chinese Remainder Theorem) Given a commutative ring A, let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be any $n \geq 2$ ideals of A such that $\mathfrak{a}_i + \mathfrak{a}_j = A$ for all $i \neq j$. Then, the homomorphism $\theta\colon A/\mathfrak{a}_1 \cdots \mathfrak{a}_n \to A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_n$ is an isomorphism.*

Proof. The map $\theta\colon A/\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n \to A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_n$ is induced by the homomorphism $\varphi\colon A \to A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_n$ given by

$$\varphi(x) = (\overline{x}_{\mathfrak{a}_1}, \ldots, \overline{x}_{\mathfrak{a}_n}).$$

Clearly, $\mathrm{Ker}\,(\varphi) = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$, so θ is well-defined and injective. We need to prove that

$$\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n$$

and that θ is surjective. We proceed by induction. The case $n = 2$ is Theorem 32.14. By induction, assume that

$$\mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_2 \cdots \mathfrak{a}_n.$$

We claim that

$$\mathfrak{a}_1 + \mathfrak{a}_2 \cdots \mathfrak{a}_n = A.$$

Indeed, since $\mathfrak{a}_1 + \mathfrak{a}_i = A$ for $i = 2, \ldots, n$, there exist some $a_i \in \mathfrak{a}_1$ and some $b_i \in \mathfrak{a}_i$ such that

$$a_i + b_i = 1, \quad i = 2, \ldots, n,$$

and by multiplying these equations, we get

$$a + b_2 \cdots b_n = 1,$$

where a is a sum of terms each containing some a_j as a factor, so $a \in \mathfrak{a}_1$ and $b_2 \cdots b_n \in \mathfrak{a}_2 \cdots \mathfrak{a}_n$, which shows that

$$\mathfrak{a}_1 + \mathfrak{a}_2 \cdots \mathfrak{a}_n = A,$$

as claimed. It follows that

$$\mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cap (\mathfrak{a}_2 \cdots \mathfrak{a}_n) = \mathfrak{a}_1 \mathfrak{a}_2 \cdots \mathfrak{a}_n.$$

Let us now prove that θ is surjective by induction. The case $n = 2$ is Theorem 32.14. Let $x_1, \ldots, x_n$ be any $n \geq 3$ elements of A. First, applying Theorem 32.14 to $\mathfrak{a}_1$ and $\mathfrak{a}_2 \cdots \mathfrak{a}_n$, we can find $y_1 \in A$ such that

$$\begin{aligned} y_1 &\equiv 1 \pmod{\mathfrak{a}_1} \\ y_1 &\equiv 0 \pmod{\mathfrak{a}_2 \cdots \mathfrak{a}_n}. \end{aligned}$$

By the induction hypothesis, we can find $y_2, \ldots, y_n \in A$ such that for all i, j with $2 \leq i, j \leq n$,

$$\begin{aligned} y_i &\equiv 1 \pmod{\mathfrak{a}_i} \\ y_i &\equiv 0 \pmod{\mathfrak{a}_j}, \quad j \neq i. \end{aligned}$$

We claim that

$$x = x_1y_1 + x_2y_2 + \cdots + x_ny_n$$

works. Indeed, using the above congruences, for $i = 2, \ldots, n$, we get

$$x \equiv x_1y_1 + x_i \pmod{\mathfrak{a}_i}, \tag{$*$}$$

but since $\mathfrak{a}_2 \cdots \mathfrak{a}_n \subseteq \mathfrak{a}_i$ for $i = 2, \ldots, n$ and $y_1 \equiv 0 \pmod{\mathfrak{a}_2 \cdots \mathfrak{a}_n}$, we have

$$x_1y_1 \equiv 0 \pmod{\mathfrak{a}_i}, \quad i = 2, \ldots, n$$

and equation $(*)$ reduces to

$$x \equiv x_i \pmod{\mathfrak{a}_i}, \quad i = 2, \ldots, n.$$

For $i = 1$, we get

$$x \equiv x_1 \pmod{\mathfrak{a}_1},$$

therefore

$$x \equiv x_i \pmod{\mathfrak{a}_i}, \quad i = 1, \ldots, n.$$

proving surjectivity. □

The classical version of the Chinese Remainder Theorem is the case where $A = \mathbb{Z}$ and where the ideals $\mathfrak{a}_i$ are defined by n pairwise relatively prime integers $m_1, \ldots, m_n$. By the Bezout identity, since m_i and m_j are relatively prime whenever $i \neq j$, there exist some $u_i, u_j \in \mathbb{Z}$ such that $u_im_i + u_jm_j = 1$, and so $m_i\mathbb{Z} + m_j\mathbb{Z} = \mathbb{Z}$. In this case, we get an isomorphism

$$\mathbb{Z}/(m_1 \cdots m_n)\mathbb{Z} \approx \prod_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z}.$$

In particular, if m is an integer greater than 1 and

$$m = \prod_i p_i^{r_i}$$

is its factorization into prime factors, then

$$\mathbb{Z}/m\mathbb{Z} \approx \prod_i \mathbb{Z}/p_i^{r_i}\mathbb{Z}.$$

In the previous situation where the integers $m_1, \ldots, m_n$ are pairwise relatively prime, if we write $m = m_1 \cdots m_n$ and $m_i' = m/m_i$ for $i = 1 \ldots, n$, then m_i and m_i' are relatively prime, and so m_i' has an inverse modulo m_i. If t_i is such an inverse, so that

$$m_i't_i \equiv 1 \pmod{m_i},$$

then it is not hard to show that for any $a_1, \ldots, a_n \in \mathbb{Z}$,

$$x = a_1 t_1 m_1' + \cdots + a_n t_n m_n'$$

satisfies the congruences

$$x \equiv a_i \pmod{m_i}, \quad i = 1, \ldots, n.$$

Theorem 32.15 can be used to characterize rings isomorphic to finite products of quotient rings. Such rings play a role in the structure theorem for torsion modules over a PID.

Given n rings $A_1, \ldots, A_n$, recall that the product ring $A = A_1 \times \cdots \times A_n$ is the ring in which addition and multiplication are defined componenwise. That is,

$$\begin{aligned}(a_1, \ldots, a_n) + (b_1, \ldots, b_n) &= (a_1 + b_1, \ldots, a_n + b_n)\\ (a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) &= (a_1 b_1, \ldots, a_n b_n).\end{aligned}$$

The additive identity is $0_A = (0, \ldots, 0)$ and the multiplicative identity is $1_A = (1, \ldots, 1)$. Then, for $i = 1, \ldots, n$, we can define the element $e_i \in A$ as follows:

$$e_i = (0, \ldots, 0, 1, 0, \ldots, 0),$$

where the 1 occurs in position i. Observe that the following properties hold for all $i, j = 1, \ldots, n$:

$$\begin{aligned} e_i^2 &= e_i\\ e_i e_j &= 0, \quad i \neq j\\ e_1 + \cdots + e_n &= 1_A. \end{aligned}$$

Also, for any element $a = (a_1, \ldots, a_n) \in A$, we have

$$e_i a = (0, \ldots, 0, a_i, 0, \ldots, 0) = pr_i(a),$$

where pr_i is the projection of A onto A_i. As a consequence

$$\mathrm{Ker}\,(pr_i) = (1_A - e_i)A.$$

Definition 32.3. Given a commutative ring A, a *direct decomposition* of A is a sequence $(\mathfrak{b}_1, \ldots, \mathfrak{b}_n)$ of ideals in A such that there is an isomorphism $A \approx A/\mathfrak{b}_1 \times \cdots \times A/\mathfrak{b}_n$.

The following theorem gives useful conditions characterizing direct decompositions of a ring.

Theorem 32.16. *Let A be a commutative ring and let $(\mathfrak{b}_1, \ldots, \mathfrak{b}_n)$ be a sequence of ideals in A. The following conditions are equivalent:*

(a) The sequence $(\mathfrak{b}_1, \ldots, \mathfrak{b}_n)$ is a direct decomposition of A.

(b) *There exist some elements* $e_1, \ldots, e_n$ *of* A *such that*

$$\begin{aligned} e_i^2 &= e_i \\ e_ie_j &= 0, \quad i \neq j \\ e_1 + \cdots + e_n &= 1_A, \end{aligned}$$

and $\mathfrak{b}_i = (1_A - e_i)A$, *for* $i, j = 1, \ldots, n$.

(c) *We have* $\mathfrak{b}_i + \mathfrak{b}_j = A$ *for all* $i \neq j$, *and* $\mathfrak{b}_1 \cdots \mathfrak{b}_n = (0)$.

(d) *We have* $\mathfrak{b}_i + \mathfrak{b}_j = A$ *for all* $i \neq j$, *and* $\mathfrak{b}_1 \cap \cdots \cap \mathfrak{b}_n = (0)$.

Proof. Assume (a). Since we have an isomorphism $A \approx A/\mathfrak{b}_1 \times \cdots \times A/\mathfrak{b}_n$, we may identify A with $A/\mathfrak{b}_1 \times \cdots \times A/\mathfrak{b}_n$, and $\mathfrak{b}_\mathfrak{i}$ with $\mathrm{Ker}\,(pr_i)$. Then, $e_1, \ldots, e_n$ are the elements defined just before Definition 32.3. As noted, $\mathfrak{b}_i = \mathrm{Ker}\,(pr_i) = (1_A - e_i)A$. This proves (b).

Assume (b). Since $\mathfrak{b}_i = (1_A - e_i)A$ and A is a ring with unit 1_A, we have $1_A - e_i \in \mathfrak{b}_i$ for $i = 1, \ldots, n$. For all $i \neq j$, we also have $e_i(1_A - e_j) = e_i - e_ie_j = e_i$, so (because $\mathfrak{b}_j$ is an ideal), $e_i \in \mathfrak{b}_j$, and thus, $1_A = 1_A - e_i + e_i \in \mathfrak{b}_\mathfrak{i} + \mathfrak{b}_j$, which shows that $\mathfrak{b}_i + \mathfrak{b}_j = A$ for all $i \neq j$. Furthermore, for any $x_i \in A$, with $1 \leq i \leq n$, we have

$$\begin{aligned} \prod_{i=1}^n x_i(1_A - e_i) &= \left(\prod_{i=1}^n x_i\right) \prod_{i=1}^n (1_A - e_i) \\ &= \left(\prod_{i=1}^n x_i\right)(1_A - \sum_{i=1}^n e_i) \\ &= 0, \end{aligned}$$

which proves that $\mathfrak{b}_1 \cdots \mathfrak{b}_n = (0)$. Thus, (c) holds.

The equivalence of (c) and (d) follows from the proof of Theorem 32.15.

The fact that (c) implies (a) is an immediate consequence of Theorem 32.15. □

Here is example of Theorem 32.16. Take the commutative ring of residue classes mod 30, namely

$$A := \mathbb{Z}/30\mathbb{Z} = \{\bar{i}\}_{i=0}^{29}.$$

Let

$$\begin{aligned} \mathfrak{b}_1 &= 2\mathbb{Z}/30\mathbb{Z} := \{2\bar{i}\}_{i=0}^{14} \\ \mathfrak{b}_2 &= 3\mathbb{Z}/30\mathbb{Z} := \{3\bar{i}\}_{i=0}^{9} \\ \mathfrak{b}_3 &= 5\mathbb{Z}/30\mathbb{Z} := \{5\bar{i}\}_{i=0}^{5}. \end{aligned}$$

Each $\mathfrak{b}_i$ is an ideal in $\mathbb{Z}/30\mathbb{Z}$. Furthermore

$$\mathbb{Z}/30\mathbb{Z} = (\mathbb{Z}/30\mathbb{Z})/(2\mathbb{Z}/30\mathbb{Z}) \times (\mathbb{Z}/30\mathbb{Z})/(3\mathbb{Z}/30\mathbb{Z}) \times (\mathbb{Z}/30\mathbb{Z})/(5\mathbb{Z}/30\mathbb{Z}),$$

where

$$e_1 = (1,0,0) \to \overline{15}, \qquad e_2 = (0,1,0) \to \overline{10}, \qquad e_3 = (0,0,1) \to \overline{6},$$

since

$$\begin{aligned} \overline{15}^2 = \overline{15}, \qquad \overline{10}^2 = \overline{10}, \qquad \overline{6}^2 = \overline{6} \\ \overline{15}\,\overline{10} = \overline{15}\,\overline{6} = \overline{10}\,\overline{6} = 0, \qquad \overline{15} + \overline{10} + \overline{6} = \overline{1}. \end{aligned}$$

Note that $\overline{15}$ corresponds to $\overline{1} \in (\mathbb{Z}/30\mathbb{Z})/(2\mathbb{Z}/30\mathbb{Z})$, $\overline{10}$ corresponds to $\overline{1} \in (\mathbb{Z}/30\mathbb{Z})/(3\mathbb{Z}/30\mathbb{Z})$, while $\overline{6}$ corresponds to $\overline{1} \in (\mathbb{Z}/30\mathbb{Z})/(5\mathbb{Z}/30\mathbb{Z})$.

32.3 Noetherian Rings and Hilbert's Basis Theorem

Given a (commutative) ring A (with unit element 1), an ideal $\mathfrak{A} \subseteq A$ is said to be *finitely generated* if there exists a finite set $\{a_1, \ldots, a_n\}$ of elements from $\mathfrak{A}$ so that

$$\mathfrak{A} = (a_1, \ldots, a_n) = \{\lambda_1 a_1 + \cdots + \lambda_n a_n \mid \lambda_i \in A,\ 1 \leq i \leq n\}.$$

If K is a field, it turns out that every polynomial ideal $\mathfrak{A}$ in $K[X_1, \ldots, X_m]$ is finitely generated. This fact due to Hilbert and known as Hilbert's basis theorem, has very important consequences. For example, in algebraic geometry, one is interested in the zero locus of a set of polyomial equations, i.e., the set, $V(\mathcal{P})$, of n-tuples $(\lambda_1, \ldots, \lambda_n) \in K^n$ so that

$$P_i(\lambda_1, \ldots, \lambda_n) = 0$$

for all polynomials $P_i(X_1, \ldots, X_n)$ in some given family, $\mathcal{P} = (P_i)_{i \in I}$. However, it is clear that

$$V(\mathcal{P}) = V(\mathfrak{A}),$$

where $\mathfrak{A}$ is the ideal generated by $\mathcal{P}$. Then, Hilbert's basis theorem says that $V(\mathfrak{A})$ is actually defined by a *finite* number of polynomials (any set of generators of $\mathfrak{A}$), even if $\mathcal{P}$ is infinite.

The property that every ideal in a ring is finitely generated is equivalent to other natural properties, one of which is the so-called *ascending chain condition*, abbreviated *a.c.c.* Before proving Hilbert's basis theorem, we explore the equivalence of these conditions.

Definition 32.4. Let A be a commutative ring with unit 1. We say that A satisfies the *ascending chain condition*, for short, the *a.c.c*, if for every ascending chain of ideals

$$\mathfrak{A}_1 \subseteq \mathfrak{A}_2 \subseteq \cdots \subseteq \mathfrak{A}_i \subseteq \cdots,$$

there is some integer $n \geq 1$ so that

$$\mathfrak{A}_i = \mathfrak{A}_n \quad \text{for all} \quad i \geq n+1.$$

We say that A satisfies the *maximum condition* if every nonempty collection C of ideals in A has a maximal element, i.e., there is some ideal $\mathfrak{A} \in C$ which is not contained in any other ideal in C.

Proposition 32.17. *A ring A satisfies the a.c.c if and only if it satisfies the maximum condition.*

Proof. Suppose that A does not satisfy the a.c.c. Then, there is an infinite strictly ascending sequence of ideals

$$\mathfrak{A}_1 \subset \mathfrak{A}_2 \subset \cdots \subset \mathfrak{A}_i \subset \cdots,$$

and the collection $C = \{\mathfrak{A}_i\}$ has no maximal element.

Conversely, assume that A satisfies the a.c.c. Let C be a nonempty collection of ideals Since C is nonempty, we may pick some ideal $\mathfrak{A}_1$ in C. If $\mathfrak{A}_1$ is not maximal, then there is some ideal $\mathfrak{A}_2$ in C so that

$$\mathfrak{A}_1 \subset \mathfrak{A}_2.$$

Using this process, if C has no maximal element, we can define by induction an infinite strictly increasing sequence

$$\mathfrak{A}_1 \subset \mathfrak{A}_2 \subset \cdots \subset \mathfrak{A}_i \subset \cdots.$$

However, the a.c.c. implies that such a sequence cannot exist. Therefore, C has a maximal element. □

Having shown that the a.c.c. condition is equivalent to the maximal condition, we now prove that the a.c.c. condition is equivalent to the fact that every ideal is finitely generated.

Proposition 32.18. *A ring A satisfies the a.c.c if and only if every ideal is finitely generated.*

Proof. Assume that every ideal is finitely generated. Consider an ascending sequence of ideals

$$\mathfrak{A}_1 \subseteq \mathfrak{A}_2 \subseteq \cdots \subseteq \mathfrak{A}_i \subseteq \cdots.$$

Observe that $\mathfrak{A} = \bigcup_i \mathfrak{A}_i$ is also an ideal. By hypothesis, $\mathfrak{A}$ has a finite generating set $\{a_1, \ldots, a_n\}$. By definition of $\mathfrak{A}$, each a_i belongs to some $\mathfrak{A}_{j_i}$, and since the $\mathfrak{A}_i$ form an ascending chain, there is some m so that $a_i \in \mathfrak{A}_m$ for $i = 1, \ldots, n$. But then,

$$\mathfrak{A}_i = \mathfrak{A}_m$$

for all $i \geq m+1$, and the a.c.c. holds.

Conversely, assume that the a.c.c. holds. Let $\mathfrak{A}$ be any ideal in A and consider the family C of subideals of $\mathfrak{A}$ that are finitely generated. The family C is nonempty, since (0) is a subideal of $\mathfrak{A}$. By Proposition 32.17, the family C has some maximal element, say $\mathfrak{B}$. For any $a \in \mathfrak{A}$, the ideal $\mathfrak{B} + (a)$ (where $\mathfrak{B} + (a) = \{b + \lambda a \mid b \in \mathfrak{B},\ \lambda \in A\}$) is also finitely generated (since $\mathfrak{B}$ is finitely generated), and by maximality, we have

$$\mathfrak{B} = \mathfrak{B} + (a).$$

So, we get $a \in \mathfrak{B}$ for all $a \in \mathfrak{A}$, and thus, $\mathfrak{A} = \mathfrak{B}$, and $\mathfrak{A}$ is finitely generated. □

Definition 32.5. A commutative ring A (with unit 1) is called *noetherian* if it satisfies the a.c.c. condition. A *noetherian domain* is a noetherian ring that is also a domain.

By Proposition 32.17 and Proposition 32.18, a noetherian ring can also be defined as a ring that either satisfies the maximal property or such that every ideal is finitely generated. The proof of Hilbert's basis theorem will make use the following lemma:

Lemma 32.19. *Let A be a (commutative) ring. For every ideal $\mathfrak{A}$ in $A[X]$, for every $i \geq 0$, let $L_i(\mathfrak{A})$ denote the set of elements of A consisting of 0 and of the coefficients of X^i in all the polynomials $f(X) \in \mathfrak{A}$ which are of degree i. Then, the $L_i(\mathfrak{A})$'s form an ascending chain of ideals in A. Furthermore, if $\mathfrak{B}$ is any ideal of $A[X]$ so that $\mathfrak{A} \subseteq \mathfrak{B}$ and if $L_i(\mathfrak{A}) = L_i(\mathfrak{B})$ for all $i \geq 0$, then $\mathfrak{A} = \mathfrak{B}$.*

Proof. That $L_i(\mathfrak{A})$ is an ideal and that $L_i(\mathfrak{A}) \subseteq L_{i+1}(\mathfrak{A})$ follows from the fact that if $f(X) \in \mathfrak{A}$ and $g(X) \in \mathfrak{A}$, then $f(X) + g(X)$, $\lambda f(X)$, and $Xf(X)$ all belong to $\mathfrak{A}$. Now, let $g(X)$ be any polynomial in $\mathfrak{B}$, and assume that $g(X)$ has degree n. Since $L_n(\mathfrak{A}) = L_n(\mathfrak{B})$, there is some polynomial $f_n(X)$ in $\mathfrak{A}$, of degree n, so that $g(X) - f_n(X)$ is of degree at most $n - 1$. Now, since $\mathfrak{A} \subseteq \mathfrak{B}$, the polynomial $g(X) - f_n(X)$ belongs to $\mathfrak{B}$. Using this process, we can define by induction a sequence of polynomials $f_{n+i}(X) \in \mathfrak{A}$, so that each $f_{n+i}(X)$ is either zero or has degree $n - i$, and

$$g(X) - (f_n(X) + f_{n+1}(X) + \cdots + f_{n+i}(X))$$

is of degree at most $n - i - 1$. Note that this last polynomial must be zero when $i = n$, and thus, $g(X) \in \mathfrak{A}$. □

We now prove Hilbert's basis theorem. The proof is substantially Hilbert's original proof. A slightly shorter proof can be given but it is not as transparent as Hilbert's proof (see the remark just after the proof of Theorem 32.20, and Zariski and Samuel [192], Chapter IV, Section 1, Theorem 1).

Theorem 32.20. *(Hilbert's basis theorem) If A is a noetherian ring, then $A[X]$ is also a noetherian ring.*

Proof. Let $\mathfrak{A}$ be any ideal in $A[X]$, and denote by $\mathcal{L}$ the set of elements of A consisting of 0 and of all the coefficients of the highest degree terms of all the polynomials in $\mathfrak{A}$. Observe that

$$\mathcal{L} = \bigcup_i L_i(\mathfrak{A}).$$

Thus, $\mathcal{L}$ is an ideal in A (this can also be proved directly). Since A is noetherian, $\mathcal{L}$ is finitely generated, and let $\{a_1, \ldots, a_n\}$ be a set of generators of $\mathcal{L}$. Let $f_1(X), \ldots, f_n(X)$ be polynomials in $\mathfrak{A}$ having respectively $a_1, \ldots, a_n$ as highest degree term coefficients. These polynomials generate an ideal $\mathfrak{B}$. Let q be the maximum of the degrees of the $f_i(X)$'s. Now, pick any polynomial $g(X) \in \mathfrak{A}$ of degree $d \geq q$, and let aX^d be its term of highest degree. Since $a \in \mathcal{L}$, we have

$$a = \lambda_1 a_1 + \cdots + \lambda_n a_n,$$

for some $\lambda_i \in A$. Consider the polynomial

$$g_1(X) = \sum_{i=1}^{n} \lambda_i f_i(X) X^{d-d_i},$$

where d_i is the degree of $f_i(X)$. Now, $g(X) - g_1(X)$ is a polynomial in $\mathfrak{A}$ of degree at most $d-1$. By repeating this procedure, we get a sequence of polynomials $g_i(X)$ in $\mathfrak{B}$, having strictly decreasing degrees, and such that the polynomial

$$g(X) - (g_1(X) + \cdots + g_i(X))$$

is of degree at most $d - i$. This polynomial must be of degree at most $q - 1$ as soon as $i = d - q + 1$. Thus, we proved that every polynomial in $\mathfrak{A}$ of degree $d \geq q$ belongs to $\mathfrak{B}$.

It remains to take care of the polynomials in $\mathfrak{A}$ of degree at most $q - 1$. Since A is noetherian, each ideal $L_i(\mathfrak{A})$ is finitely generated, and let $\{a_{i1}, \ldots, a_{in_i}\}$ be a set of generators for $L_i(\mathfrak{A})$ (for $i = 0, \ldots, q-1$). Let $f_{ij}(X)$ be a polynomial in $\mathfrak{A}$ having $a_{ij}X^i$ as its highest degree term. Given any polynomial $g(X) \in \mathfrak{A}$ of degree $d \leq q-1$, if we denote its term of highest degree by aX^d, then, as in the previous argument, we can write

$$a = \lambda_1 a_{d1} + \cdots + \lambda_{n_d} a_{dn_d},$$

and we define

$$g_1(X) = \sum_{i=1}^{n_d} \lambda_i f_{di}(X) X^{d-d_i},$$

where d_i is the degree of $f_{di}(X)$. Then, $g(X) - g_1(X)$ is a polynomial in $\mathfrak{A}$ of degree at most $d-1$, and by repeating this procedure at most q times, we get an element of $\mathfrak{A}$ of degree 0, and the latter is a linear combination of the f_{0i}'s. This proves that every polynomial in $\mathfrak{A}$ of degree at most $q - 1$ is a combination of the polynomials $f_{ij}(X)$, for $0 \leq i \leq q-1$ and $1 \leq j \leq n_i$. Therefore, $\mathfrak{A}$ is generated by the $f_k(X)$'s and the $f_{ij}(X)$'s, a finite number of polynomials. □

Remark: Only a small part of Lemma 32.19 was used in the above proof, namely, the fact that $L_i(\mathfrak{A})$ is an ideal. A shorter proof of Theorem 32.21 making full use of Lemma 32.19 can be given as follows:

Proof. (Second proof) Let $(\mathfrak{A}_i)_{i\geq 1}$ be an ascending sequence of ideals in $A[X]$. Consider the doubly indexed family $(L_i(\mathfrak{A}_j))$ of ideals in A. Since A is noetherian, by the maximal property, this family has a maximal element $L_p(\mathfrak{A}_q)$. Since the $L_i(\mathfrak{A}_j)$'s form an ascending sequence when either i or j is fixed, we have $L_i(\mathfrak{A}_j) = L_p(\mathfrak{A}_q)$ for all i and j with $i \geq p$ and $j \geq q$, and thus, $L_i(\mathfrak{A}_q) = L_i(\mathfrak{A}_j)$ for all i and j with $i \geq p$ and $j \geq q$. On the other hand, for any fixed i, the a.c.c. shows that there exists some integer $n(i)$ so that $L_i(\mathfrak{A}_j) = L_i(\mathfrak{A}_{n(i)})$ for all $j \geq n(i)$. Since $L_i(\mathfrak{A}_q) = L_i(\mathfrak{A}_j)$ when $i \geq p$ and $j \geq q$, we may take $n(i) = q$ if $i \geq p$. This shows that there is some n_0 so that $n(i) \leq n_0$ for all $i \geq 0$, and thus, we have $L_i(\mathfrak{A}_j) = L_i(\mathfrak{A}_{n(0)})$ for every i and for every $j \geq n(0)$. By Lemma 32.19, we get $\mathfrak{A}_j = \mathfrak{A}_{n(0)}$ for every $j \geq n(0)$, establishing the fact that $A[X]$ satisfies the a.c.c. □

Using induction, we immediately obtain the following important result.

Corollary 32.21. *If A is a noetherian ring, then $A[X_1, \ldots, X_n]$ is also a noetherian ring.*

Since a field K is obviously noetherian (since it has only two ideals, (0) and K), we also have:

Corollary 32.22. *If K is a field, then $K[X_1, \ldots, X_n]$ is a noetherian ring.*

32.4 Futher Readings

The material of this Chapter is thoroughly covered in Lang [108], Artin [7], Mac Lane and Birkhoff [117], Bourbaki [25, 26], Malliavin [118], Zariski and Samuel [192], and Van Der Waerden [177].

Chapter 33

Tensor Algebras and Symmetric Algebras

Tensors are creatures that we would prefer did not exist but keep showing up whenever multilinearity manifests itself.

One of the goals of differential geometry is to be able to generalize "calculus on $\mathbb{R}^n$" to spaces more general than $\mathbb{R}^n$, namely manifolds. We would like to differentiate functions $f\colon M \to \mathbb{R}$ defined on a manifold, optimize functions (find their minima or maxima), but also to integrate such functions, as well as compute areas and volumes of subspaces of our manifold.

The suitable notion of differentiation is the notion of tangent map, a linear notion. One of the main discoveries made at the beginning of the twentieth century by Poincaré and Élie Cartan, is that the "right" approach to integration is to integrate *differential forms*, and not functions. To integrate a function f, we integrate the form $f\omega$, where ω is a *volume form* on the manifold M. The formalism of differential forms takes care of the process of the change of variables quite automatically, and allows for a very clean statement of *Stokes' formula*.

Differential forms can be combined using a notion of product called the wedge product, but what really gives power to the formalism of differential forms is the magical operation d of *exterior differentiation*. Given a form ω, we obtain another form $d\omega$, and remarkably, the following equation holds

$$dd\omega = 0.$$

As silly as it looks, the above equation lies at the core of the notion of cohomology, a powerful algebraic tool to understand the topology of manifolds, and more generally of topological spaces.

Élie Cartan had many of the intuitions that lead to the cohomology of differential forms, but it was George de Rham who defined it rigorously and proved some important theorems about it. It turns out that the notion of Laplacian can also be defined on differential forms using a device due to Hodge, and some important theorems can be obtained: the Hodge decomposition theorem, and Hodge's theorem about the isomorphism between the de Rham cohomology groups and the spaces of harmonic forms.

To understand all this, one needs to learn about differential forms, which turn out to be certain kinds of skew-symmetric (also called alternating) tensors.

If one's only goal is to define differential forms, then it is possible to take some short cuts and to avoid introducing the general notion of a tensor. However, tensors that are not necessarily skew-symmetric arise naturally, such as the curvature tensor, and in the theory of vector bundles, general tensor products are needed.

Consequently, we made the (perhaps painful) decision to provide a fairly detailed exposition of tensors, starting with arbitrary tensors, and then specializing to symmetric and alternating tensors. In particular, we explain rather carefully the process of taking the dual of a tensor (of all three flavors).

We refrained from following the approach in which a tensor is defined as a multilinear map defined on a product of dual spaces, because it seems very artificial and confusing (certainly to us). This approach relies on duality results that only hold in finite dimension, and consequently unecessarily restricts the theory of tensors to finite dimensional spaces. We also feel that it is important to begin with a coordinate-free approach. Bases can be chosen for computations, but tensor algebra should not be reduced to raising or lowering indices.

Readers who feel that they are familiar with tensors should probably skip this chapter and the next. They can come back to them "by need."

We begin by defining tensor products of vector spaces over a field and then we investigate some basic properties of these tensors, in particular the existence of bases and duality. After this we investigate special kinds of tensors, namely symmetric tensors and skew-symmetric tensors. Tensor products of modules over a commutative ring with identity will be discussed very briefly. They show up naturally when we consider the space of sections of a tensor product of vector bundles.

Given a linear map $f\colon E \to F$ (where E and F are two vector spaces over a field K), we know that if we have a basis $(u_i)_{i\in I}$ for E, then f is completely determined by its values $f(u_i)$ on the basis vectors. For a multilinear map $f\colon E^n \to F$, we don't know if there is such a nice property but it would certainly be very useful.

In many respects tensor products allow us to define multilinear maps in terms of their action on a suitable basis. The crucial idea is to *linearize*, that is, to create a new vector space $E^{\otimes n}$ such that the multilinear map $f\colon E^n \to F$ is turned into a *linear map* $f_\otimes\colon E^{\otimes n} \to F$ which is equivalent to f in a strong sense. If in addition, f is symmetric, then we can define a symmetric tensor power $\mathrm{Sym}^n(E)$, and every symmetric multilinear map $f\colon E^n \to F$ is turned into a *linear map* $f_\odot\colon \mathrm{Sym}^n(E) \to F$ which is equivalent to f in a strong sense. Similarly, if f is alternating, then we can define a skew-symmetric tensor power $\bigwedge^n(E)$, and every alternating multilinear map is turned into a *linear map* $f_\wedge\colon \bigwedge^n(E) \to F$ which is equivalent to f in a strong sense.

Tensor products can be defined in various ways, some more abstract than others. We try to stay down to earth, without excess.

Before proceeding any further, we review some facts about dual spaces and pairings. Pairings will be used to deal with dual spaces of tensors.

33.1 Linear Algebra Preliminaries: Dual Spaces and Pairings

We assume that we are dealing with vector spaces over a field K. As usual the *dual space* E^* of a vector space E is defined by $E^* = \mathrm{Hom}(E, K)$. The dual space E^* is the vector space consisting of all linear maps $\omega \colon E \to K$ with values in the field K.

A problem that comes up often is to decide when a space E is isomorphic to the dual F^* of some other space F (possibly equal to E). The notion of pairing due to Pontrjagin provides a very clean criterion.

Definition 33.1. Given two vector spaces E and F over a field K, a map $\langle -, - \rangle \colon E \times F \to K$ is a *nondegenerate pairing* iff it is bilinear and iff $\langle u, v\rangle = 0$ for all $v \in F$ implies $u = 0$, and $\langle u, v\rangle = 0$ for all $u \in E$ implies $v = 0$. A nondegenerate pairing induces two linear maps $\varphi \colon E \to F^*$ and $\psi \colon F \to E^*$ defined such that for all for all $u \in E$ and all $v \in F$, $\varphi(u)$ is the linear form in F^* and $\psi(v)$ is the linear form in E^* given by

$$\begin{aligned} \varphi(u)(y) &= \langle u, y\rangle \quad \text{for all } y \in F \\ \psi(v)(x) &= \langle x, v\rangle \quad \text{for all } x \in E. \end{aligned}$$

Schematically, $\varphi(u) = \langle u, - \rangle$ and $\psi(v) = \langle -, v\rangle$.

Proposition 33.1. *For every nondegenerate pairing $\langle -, - \rangle \colon E \times F \to K$, the induced maps $\varphi \colon E \to F^*$ and $\psi \colon F \to E^*$ are linear and injective. Furthermore, if E and F are finite dimensional, then $\varphi \colon E \to F^*$ and $\psi \colon F \to E^*$ are bijective.*

Proof. The maps $\varphi \colon E \to F^*$ and $\psi \colon F \to E^*$ are linear because $u, v \mapsto \langle u, v\rangle$ is bilinear. Assume that $\varphi(u) = 0$. This means that $\varphi(u)(y) = \langle u, y\rangle = 0$ for all $y \in F$, and as our pairing is nondegenerate, we must have $u = 0$. Similarly, ψ is injective. If E and F are finite dimensional, then $\dim(E) = \dim(E^*)$ and $\dim(F) = \dim(F^*)$. However, the injectivity of φ and ψ implies that that $\dim(E) \leq \dim(F^*)$ and $\dim(F) \leq \dim(E^*)$. Consequently $\dim(E) \leq \dim(F)$ and $\dim(F) \leq \dim(E)$, so $\dim(E) = \dim(F)$. Therefore, $\dim(E) = \dim(F^*)$ and φ is bijective (and similarly $\dim(F) = \dim(E^*)$ and ψ is bijective). □

Proposition 33.1 shows that when E and F are finite dimensional, a nondegenerate pairing induces *canonical isomorphims* $\varphi \colon E \to F^*$ and $\psi \colon F \to E^*$; that is, isomorphisms that do not depend on the choice of bases. An important special case is the case where $E = F$ and we have an inner product (a symmetric, positive definite bilinear form) on E.

Remark: When we use the term "canonical isomorphism," we mean that such an isomorphism is defined independently of any choice of bases. For example, if E is a finite dimensional vector space and $(e_1, \ldots, e_n)$ is any basis of E, we have the dual basis $(e_1^*, \ldots, e_n^*)$ of E^* (where, $e_i^*(e_j) = \delta_{i\,j}$), and thus the map $e_i \mapsto e_i^*$ is an isomorphism between E and E^*. This isomorphism is *not* canonical.

On the other hand, if $\langle -, - \rangle$ is an inner product on E, then Proposition 33.1 shows that the nondegenerate pairing $\langle -, - \rangle$ on $E \times E$ induces a canonical isomorphism between E and E^*. This isomorphism is often denoted $\flat \colon E \to E^*$, and we usually write $u^\flat$ for $\flat(u)$, with $u \in E$. Schematically, $u^\flat = \langle u, - \rangle$. The inverse of $\flat$ is denoted $\sharp \colon E^* \to E$, and given any linear form $\omega \in E^*$, we usually write $\omega^\sharp$ for $\sharp(\omega)$. Schematically, $\omega = \langle \omega^\sharp, - \rangle$.

Given any basis, $(e_1, \ldots, e_n)$ of E (not necessarily orthonormal), let (g_{ij}) be the $n \times n$-matrix given by $g_{ij} = \langle e_i, e_j \rangle$ (the *Gram* matrix of the inner product). Recall that the *dual basis* $(e_1^*, \ldots, e_n^*)$ of E^* consists of the coordinate forms $e_i^* \in E^*$, which are characterized by the following properties:

$$e_i^*(e_j) = \delta_{ij}, \quad 1 \leq i, j \leq n.$$

The inverse of the Gram matrix (g_{ij}) is often denoted by (g^{ij}) (by raising the indices).

The tradition of raising and lowering indices is pervasive in the literature on tensors. It is indeed useful to have some notational convention to distinguish between vectors and linear forms (also called *one-forms* or *covectors*). The usual convention is that coordinates of vectors are written using superscripts, as in $u = \sum_{i=1}^n u^i e_i$, and coordinates of one-forms are written using subscripts, as in $\omega = \sum_{i=1}^n \omega_i e_i^*$. Actually, since vectors are indexed with subscripts, one-forms are indexed with superscripts, so e_i^* should be written as e^i.

The motivation is that summation signs can then be omitted, according to the *Einstein summation convention*. According to this convention, whenever a summation variable (such as i) appears both as a subscript and a superscript in an expression, it is assumed that it is involved in a summation. For example the sum $\sum_{i=1}^n u^i e_i$ is abbreviated as

$$u^i e_i,$$

and the sum $\sum_{i=1}^n \omega_i e^i$ is abbreviated as

$$\omega_i e^i.$$

In this text we will not use the Einstein summation convention, which we find somewhat confusing, and we will also write e_i^* instead of e^i.

The maps $\flat$ and $\sharp$ can be described explicitly in terms of the Gram matrix of the inner product and its inverse.

Proposition 33.2. *For any vector space E, given a basis $(e_1, \ldots, e_n)$ for E and its dual basis $(e_1^*, \ldots, e_n^*)$ for E^*, for any inner product $\langle -, - \rangle$ on E, if (g_{ij}) is its Gram matrix, with*

$g_{ij} = \langle e_i, e_j\rangle$, and (g^{ij}) is its inverse, then for every vector $u = \sum_{j=1}^n u^j e_j \in E$ and every one-form $\omega = \sum_{i=1}^n \omega_i e_i^* \in E^*$, we have

$$u^\flat = \sum_{i=1}^n \omega_i e_i^*, \quad \textit{with} \quad \omega_i = \sum_{j=1}^n g_{ij} u^j,$$

and

$$\omega^\sharp = \sum_{j=1}^n (\omega^\sharp)^j e_j, \quad \textit{with} \quad (\omega^\sharp)^i = \sum_{j=1}^n g^{ij}\omega_j.$$

Proof. For every $u = \sum_{j=1}^n u^j e_j$, since $u^\flat(v) = \langle u, v\rangle$ for all $v \in E$, we have

$$u^\flat(e_i) = \langle u, e_i\rangle = \left\langle \sum_{j=1}^n u^j e_j, e_i \right\rangle = \sum_{j=1}^n u^j \langle e_j, e_i\rangle = \sum_{j=1}^n g_{ij} u^j,$$

so we get

$$u^\flat = \sum_{i=1}^n \omega_i e_i^*, \quad \text{with} \quad \omega_i = \sum_{j=1}^n g_{ij} u^j.$$

If we write $\omega \in E^*$ as $\omega = \sum_{i=1}^n \omega_i e_i^*$ and $\omega^\sharp \in E$ as $\omega^\sharp = \sum_{j=1}^n (\omega^\sharp)^j e_j$, since

$$\omega_i = \omega(e_i) = \langle \omega^\sharp, e_i\rangle = \sum_{j=1}^n (\omega^\sharp)^j g_{ij}, \qquad 1 \le i \le n,$$

we get

$$(\omega^\sharp)^i = \sum_{j=1}^n g^{ij}\omega_j,$$

where (g^{ij}) is the inverse of the matrix (g_{ij}). □

The map $\flat$ has the effect of lowering (flattening!) indices, and the map $\sharp$ has the effect of raising (sharpening!) indices.

Here is an explicit example of Proposition 33.2. Let (e_1, e_2) be a basis of E such that

$$\langle e_1, e_1\rangle = 1, \qquad \langle e_1, e_2\rangle = 2, \qquad \langle e_2, e_2\rangle = 5.$$

Then

$$g = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}, \qquad g^{-1} = \begin{pmatrix} 5 & -2 \\ -2 & 1 \end{pmatrix}.$$

Set $u = u^1 e_1 + u^2 e_2$ and observe that

$$\begin{aligned} u^\flat(e_1) &= \langle u^1 e_1 + u^2 e_2, e_1\rangle = \langle e_1, e_1\rangle u^1 + \langle e_2, e_1\rangle u^2 = g_{11}u^1 + g_{12}u^2 = u^1 + 2u^2 \\ u^\flat(e_2) &= \langle u^1 e_1 + u^2 e_2, e_2\rangle = \langle e_1, e_2\rangle u^1 + \langle e_2, e_2\rangle u^2 = g_{21}u^1 + g_{22}u^2 = 2u^1 + 5u^2, \end{aligned}$$

which in turn implies that

$$u^\flat = \omega_1 e_1^* + \omega_2 e_2^* = u^\flat(e_1)e_1^* + u^\flat(e_2)e_2^* = (u^1 + 2u^2)e_1^* + (2u^1 + 5u^2)e_2^*.$$

Given $\omega = \omega_1 e_1^* + \omega_2 e_2^*$, we calculate $\omega^\sharp = (\omega^\sharp)^1 e_1 + (\omega^\sharp)^2 e_2$ from the following two linear equalities:

$$\begin{aligned}
\omega_1 = \omega(e_1) &= \langle \omega^\sharp, e_1\rangle = \langle (\omega^\sharp)^1 e_1 + (\omega^\sharp)^2 e_2, e_1\rangle \\
&= \langle e_1, e_1\rangle (\omega^\sharp)^1 + \langle e_2, e_1\rangle (\omega^\sharp)^2 = (\omega^\sharp)^1 + 2(\omega^\sharp)^2 = g_{11}(\omega^\sharp)^1 + g_{12}(\omega^\sharp)^2 \\
\omega_2 = \omega(e_2) &= \langle \omega^\sharp, e_2\rangle = \langle (\omega^\sharp)^1 e_1 + (\omega^\sharp)^2 e_2, e_2\rangle \\
&= \langle e_1, e_2\rangle (\omega^\sharp)^1 + \langle e_2, e_2\rangle (\omega^\sharp)^2 = 2(\omega^\sharp)^1 + 5(\omega^\sharp)^2 = g_{21}(\omega^\sharp)^1 + g_{22}(\omega^\sharp)^2.
\end{aligned}$$

These equalities are concisely written as

$$\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} (\omega^\sharp)^1 \\ (\omega^\sharp)^2 \end{pmatrix} = g \begin{pmatrix} (\omega^\sharp)^1 \\ (\omega^\sharp)^2 \end{pmatrix}.$$

Then

$$\begin{pmatrix} (\omega^\sharp)^1 \\ (\omega^\sharp)^2 \end{pmatrix} = g^{-1} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} 5 & -2 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix},$$

which in turn implies

$$(\omega^\sharp)^1 = 5\omega_1 - 2\omega_2, \qquad (\omega^\sharp)^2 = -2\omega_1 + \omega_2,$$

i.e.

$$\omega^\sharp = (5\omega_1 - 2\omega_2)e_1 + (-2\omega_1 + \omega_2)e_2.$$

The inner product $\langle -, - \rangle$ on E induces an inner product on E^* denoted $\langle -, - \rangle_{E^*}$, and given by

$$\langle \omega_1, \omega_2\rangle_{E^*} = \langle \omega_1^\sharp, \omega_2^\sharp\rangle, \quad \text{for all } \omega_1, \omega_2 \in E^*.$$

Then we have

$$\langle u^\flat, v^\flat\rangle_{E^*} = \langle (u^\flat)^\sharp, (v^\flat)^\sharp\rangle = \langle u, v\rangle \quad \text{for all} \quad u, v \in E.$$

If $(e_1, \ldots, e_n)$ is a basis of E and $g_{ij} = \langle e_i, e_j\rangle$, as

$$(e_i^*)^\sharp = \sum_{k=1}^n g^{ik} e_k,$$

an easy computation shows that

$$\langle e_i^*, e_j^*\rangle_{E^*} = \langle (e_i^*)^\sharp, (e_j^*)^\sharp\rangle = g^{ij};$$

that is, in the basis $(e_1^*, \ldots, e_n^*)$, the inner product on E^* is represented by the matrix (g^{ij}), the inverse of the matrix (g_{ij}).

The inner product on a finite vector space also yields a canonical isomorphism between the space $\mathrm{Hom}(E, E; K)$ of bilinear forms on E, and the space $\mathrm{Hom}(E, E)$ of linear maps from E to itself. Using this isomorphism, we can define the trace of a bilinear form in an intrinsic manner. This technique is used in differential geometry, for example, to define the divergence of a differential one-form.

Proposition 33.3. *If $\langle -, - \rangle$ is an inner product on a finite vector space E (over a field, K), then for every bilinear form $f\colon E \times E \to K$, there is a unique linear map $f^\natural\colon E \to E$ such that*

$$f(u, v) = \langle f^\natural(u), v \rangle, \quad \textit{for all } u, v \in E.$$

The map $f \mapsto f^\natural$ is a linear isomorphism between $\mathrm{Hom}(E, E; K)$ *and* $\mathrm{Hom}(E, E)$.

Proof. For every $g \in \mathrm{Hom}(E, E)$, the map given by

$$f(u, v) = \langle g(u), v \rangle, \quad u, v \in E,$$

is clearly bilinear. It is also clear that the above defines a linear map from $\mathrm{Hom}(E, E)$ to $\mathrm{Hom}(E, E; K)$. This map is injective, because if $f(u, v) = 0$ for all $u, v \in E$, as $\langle -, - \rangle$ is an inner product, we get $g(u) = 0$ for all $u \in E$. Furthermore, both spaces $\mathrm{Hom}(E, E)$ and $\mathrm{Hom}(E, E; K)$ have the same dimension, so our linear map is an isomorphism. □

If $(e_1, \ldots, e_n)$ is an orthonormal basis of E, then we check immediately that the trace of a linear map g (which is independent of the choice of a basis) is given by

$$\mathrm{tr}(g) = \sum_{i=1}^{n} \langle g(e_i), e_i \rangle,$$

where $n = \dim(E)$.

Definition 33.2. We define the *trace of the bilinear form f* by

$$\mathrm{tr}(f) = \mathrm{tr}(f^\natural).$$

From Proposition 33.3, $\mathrm{tr}(f)$ is given by

$$\mathrm{tr}(f) = \sum_{i=1}^{n} f(e_i, e_i),$$

for any orthonormal basis $(e_1, \ldots, e_n)$ of E. We can also check directly that the above expression is independent of the choice of an orthonormal basis.

We demonstrate how to calculate $\mathrm{tr}(f)$ where $f : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$ with $f((x_1, y_1), (x_2, y_2)) = x_1x_2 + 2x_2y_1 + 3x_1y_2 - y_1y_2$. Under the standard basis for $\mathbb{R}^2$, the bilinear form f is represented as

$$\begin{pmatrix} x_1 & y_1 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}.$$

This matrix representation shows that

$$f^\natural = \begin{pmatrix} 1 & 3 \\ 2 & -1 \end{pmatrix}^\top = \begin{pmatrix} 1 & 2 \\ 3 & -1 \end{pmatrix},$$

and hence

$$\mathrm{tr}(f) = \mathrm{tr}(f^\natural) = \mathrm{tr} \begin{pmatrix} 1 & 2 \\ 3 & -1 \end{pmatrix} = 0.$$

We will also need the following proposition to show that various families are linearly independent.

Proposition 33.4. *Let E and F be two nontrivial vector spaces and let $(u_i)_{i\in I}$ be any family of vectors $u_i \in E$. The family $(u_i)_{i\in I}$ is linearly independent iff for every family $(v_i)_{i\in I}$ of vectors $v_i \in F$, there is some linear map $f\colon E \to F$ so that $f(u_i) = v_i$ for all $i \in I$.*

Proof. Left as an exercise. □

33.2 Tensors Products

First we define tensor products, and then we prove their existence and uniqueness up to isomorphism.

Definition 33.3. Let K be a given field, and let $E_1, \ldots, E_n$ be $n \geq 2$ given vector spaces. For any vector space F, a map $f\colon E_1 \times \cdots \times E_n \to F$ is *multilinear* iff it is linear in each of its argument; that is,

$$\begin{aligned} f(u_1, \ldots u_{i_1}, v + w, u_{i+1}, \ldots, u_n) &= f(u_1, \ldots u_{i_1}, v, u_{i+1}, \ldots, u_n) \\ &\quad + f(u_1, \ldots u_{i_1}, w, u_{i+1}, \ldots, u_n) \\ f(u_1, \ldots u_{i_1}, \lambda v, u_{i+1}, \ldots, u_n) &= \lambda f(u_1, \ldots u_{i_1}, v, u_{i+1}, \ldots, u_n), \end{aligned}$$

for all $u_j \in E_j$ $(j \neq i)$, all $v, w \in E_i$ and all $\lambda \in K$, for $i = 1 \ldots, n$.

The set of multilinear maps as above forms a vector space denoted $\mathrm{L}(E_1, \ldots, E_n; F)$ or $\mathrm{Hom}(E_1, \ldots, E_n; F)$. When $n = 1$, we have the vector space of linear maps $\mathrm{L}(E, F)$ (also denoted $\mathrm{Hom}(E, F)$). (To be very precise, we write $\mathrm{Hom}_K(E_1, \ldots, E_n; F)$ and $\mathrm{Hom}_K(E, F)$.)

Definition 33.4. A *tensor product* of $n \geq 2$ vector spaces $E_1, \ldots, E_n$ is a vector space T together with a multilinear map $\varphi\colon E_1 \times \cdots \times E_n \to T$, such that for every vector space F and for every multilinear map $f\colon E_1 \times \cdots \times E_n \to F$, there is a unique linear map $f_\otimes\colon T \to F$ with

$$f(u_1, \ldots, u_n) = f_\otimes(\varphi(u_1, \ldots, u_n)),$$

for all $u_1 \in E_1, \ldots, u_n \in E_n$, or for short

$$f = f_\otimes \circ \varphi.$$

Equivalently, there is a unique linear map $f_\otimes$ such that the following diagram commutes.

$$\begin{tikzcd}
E_1 \times \cdots \times E_n \arrow[r, "\varphi"] \arrow[dr, "f"'] & T \arrow[d, "f_\otimes"] \\
& F
\end{tikzcd}$$

The above property is called the *universal mapping property* of the tensor product (T, φ).

We show that any two tensor products (T_1, φ_1) and (T_2, φ_2) for $E_1, \ldots, E_n$, are isomorphic.

Proposition 33.5. *Given any two tensor products (T_1, φ_1) and (T_2, φ_2) for $E_1, \ldots, E_n$, there is an isomorphism $h\colon T_1 \to T_2$ such that*

$$\varphi_2 = h \circ \varphi_1.$$

Proof. Focusing on (T_1, φ_1), we have a multilinear map $\varphi_2\colon E_1 \times \cdots \times E_n \to T_2$, and thus there is a unique linear map $(\varphi_2)_\otimes\colon T_1 \to T_2$ with

$$\varphi_2 = (\varphi_2)_\otimes \circ \varphi_1$$

as illustrated by the following commutative diagram.

$$\begin{tikzcd}
E_1 \times \cdots \times E_n \arrow[r, "\varphi_1"] \arrow[dr, "\varphi_2"'] & T_1 \arrow[d, "(\varphi_2)_\otimes"] \\
& T_2
\end{tikzcd}$$

Similarly, focusing now on on (T_2, φ_2), we have a multilinear map $\varphi_1\colon E_1 \times \cdots \times E_n \to T_1$, and thus there is a unique linear map $(\varphi_1)_\otimes\colon T_2 \to T_1$ with

$$\varphi_1 = (\varphi_1)_\otimes \circ \varphi_2$$

as illustrated by the following commutative diagram.

$$\begin{tikzcd}
E_1 \times \cdots \times E_n \arrow[r, "\varphi_2"] \arrow[dr, "\varphi_1"'] & T_2 \arrow[d, "(\varphi_1)_{\otimes}"] \\
& T_1
\end{tikzcd}$$

Putting these diagrams together, we obtain the commutative diagrams

$$\begin{tikzcd}
& T_1 \arrow[d, "(\varphi_2)_{\otimes}"] \\
E_1 \times \cdots \times E_n \arrow[ur, "\varphi_1"] \arrow[r, "\varphi_2"] \arrow[dr, "\varphi_1"'] & T_2 \arrow[d, "(\varphi_1)_{\otimes}"] \\
& T_1
\end{tikzcd}$$

and

$$\begin{tikzcd}
& T_2 \arrow[d, "(\varphi_1)_{\otimes}"] \\
E_1 \times \cdots \times E_n \arrow[ur, "\varphi_2"] \arrow[r, "\varphi_1"] \arrow[dr, "\varphi_2"'] & T_1 \arrow[d, "(\varphi_2)_{\otimes}"] \\
& T_2,
\end{tikzcd}$$

which means that

$$\varphi_1 = (\varphi_1)_{\otimes} \circ (\varphi_2)_{\otimes} \circ \varphi_1 \quad \text{and} \quad \varphi_2 = (\varphi_2)_{\otimes} \circ (\varphi_1)_{\otimes} \circ \varphi_2.$$

On the other hand, focusing on (T_1, φ_1), we have a multilinear map $\varphi_1\colon E_1 \times \cdots \times E_n \to T_1$, but the unique linear map $h\colon T_1 \to T_1$ with

$$\varphi_1 = h \circ \varphi_1$$

is $h = \mathrm{id}$, as illustrated by the following commutative diagram

$$\begin{tikzcd}
E_1 \times \cdots \times E_n \arrow[r, "\varphi_1"] \arrow[dr, "\varphi_1"'] & T_1 \arrow[d, "\mathrm{id}"] \\
& T_1,
\end{tikzcd}$$

and since $(\varphi_1)_{\otimes} \circ (\varphi_2)_{\otimes}$ is linear as a composition of linear maps, we must have

$$(\varphi_1)_{\otimes} \circ (\varphi_2)_{\otimes} = \mathrm{id}.$$

Similarly, we have the commutative diagram

$$\begin{tikzcd}
E_1 \times \cdots \times E_n \arrow[r, "\varphi_2"] \arrow[dr, "\varphi_2"'] & T_2 \arrow[d, "\mathrm{id}"] \\
& T_2,
\end{tikzcd}$$

and we must have

$$(\varphi_2)_\otimes \circ (\varphi_1)_\otimes = \mathrm{id}.$$

This shows that $(\varphi_1)_\otimes$ and $(\varphi_2)_\otimes$ are inverse linear maps, and thus, $(\varphi_2)_\otimes \colon T_1 \to T_2$ is an isomorphism between T_1 and T_2. □

Now that we have shown that tensor products are unique up to isomorphism, we give a construction that produces them. Tensor products are obtained from free vector spaces by a quotient process, so let us begin by describing the construction of the free vector space generated by a set.

For simplicity assume that our set I is finite, say

$$I = \{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\}.$$

The construction works for any field K (and in fact for any commutative ring A, in which case we obtain the free A-module generated by I). Assume that $K = \mathbb{R}$. The *free vector space generated by I* is the set of all formal linear combinations of the form

$$a\heartsuit + b\diamondsuit + c\spadesuit + d\clubsuit,$$

with $a, b, c, d \in \mathbb{R}$. It is assumed that the order of the terms does not matter. For example,

$$2\heartsuit - 5\diamondsuit + 3\spadesuit = -5\diamondsuit + 2\heartsuit + 3\spadesuit.$$

Addition and multiplication by a scalar are are defined as follows:

$$\begin{aligned}(a_1\heartsuit + b_1\diamondsuit + c_1\spadesuit + d_1\clubsuit) &+ (a_2\heartsuit + b_2\diamondsuit + c_2\spadesuit + d_2\clubsuit)\\ &= (a_1 + a_2)\heartsuit + (b_1 + b_2)\diamondsuit + (c_1 + c_2)\spadesuit + (d_1 + d_2)\clubsuit,\end{aligned}$$

and

$$\alpha \cdot (a\heartsuit + b\diamondsuit + c\spadesuit + d\clubsuit) = \alpha a\heartsuit + \alpha b\diamondsuit + \alpha c\spadesuit + \alpha d\clubsuit,$$

for all $a, b, c, d, \alpha \in \mathbb{R}$. With these operations, it is immediately verified that we obtain a vector space denoted $\mathbb{R}^{(I)}$. The set I can be viewed as embedded in $\mathbb{R}^{(I)}$ by the injection ι given by

$$\iota(\heartsuit) = 1\heartsuit, \quad \iota(\diamondsuit) = 1\diamondsuit, \quad \iota(\spadesuit) = 1\spadesuit, \quad \iota(\clubsuit) = 1\clubsuit.$$

Thus, $\mathbb{R}^{(I)}$ can be viewed as the vector space with the special basis $I = \{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\}$. In our case, $\mathbb{R}^{(I)}$ is isomorophic to $\mathbb{R}^4$.

The exact same construction works for any field K, and we obtain a vector space denoted by $K^{(I)}$ and an injection $\iota\colon I \to K^{(I)}$.

The main reason why the free vector space $K^{(I)}$ over a set I is interesting is that it satisfies a *universal mapping property*. This means that for every vector space F (over the field K), any function $h\colon I \to F$, where F is *considered just a set*, has a unique linear extension $\overline{h}\colon K^{(I)} \to F$. By extension, we mean that $\overline{h}(i) = h(i)$ for all $i \in I$, or more rigorously that $h = \overline{h} \circ \iota$.

For example, if $I = \{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\}$, $K = \mathbb{R}$, and $F = \mathbb{R}^3$, the function h given by

$$h(\heartsuit) = (1,1,1), \quad h(\diamondsuit) = (1,1,0), \quad h(\spadesuit) = (1,0,0), \quad h(\clubsuit) = (0, 0-1)$$

has a unique linear extension $\overline{h}\colon \mathbb{R}^{(I)} \to \mathbb{R}^3$ to the free vector space $\mathbb{R}^{(I)}$, given by

$$\begin{aligned}
\overline{h}(a\heartsuit + b\diamondsuit + c\spadesuit + d\clubsuit) &= a\overline{h}(\heartsuit) + b\overline{h}(\diamondsuit) + c\overline{h}(\spadesuit) + d\overline{h}(\clubsuit) \\
&= ah(\heartsuit) + bh(\diamondsuit) + ch(\spadesuit) + dh(\clubsuit) \\
&= a(1,1,1) + b(1,1,0) + c(1,0,0) + d(0,0,-1) \\
&= (a+b+c, a+b, a-d).
\end{aligned}$$

To generalize the construction of a free vector space to infinite sets I, we observe that the formal linear combination $a\heartsuit + b\diamondsuit + c\spadesuit + d\clubsuit$ can be viewed as the function $f\colon I \to \mathbb{R}$ given by

$$f(\heartsuit) = a, \quad f(\diamondsuit) = b, \quad f(\spadesuit) = c, \quad f(\clubsuit) = d,$$

where $a, b, c, d \in \mathbb{R}$. More generally, we can replace $\mathbb{R}$ by any field K. If I is finite, then the set of all such functions is a vector space under pointwise addition and pointwise scalar multiplication. If I is infinite, since addition and scalar multiplication only makes sense for finite vectors, we require that our functions $f\colon I \to K$ take the value 0 except for possibly finitely many arguments. We can think of such functions as an infinite sequences $(f_i)_{i\in I}$ of elements f_i of K indexed by I, with only finitely many nonzero f_i. The formalization of this construction goes as follows.

Given any set I viewed as an index set, let $K^{(I)}$ be the set of all functions $f\colon I \to K$ such that $f(i) \neq 0$ only for finitely many $i \in I$. As usual, denote such a function by $(f_i)_{i\in I}$; it is a family of finite support. We make $K^{(I)}$ into a vector space by defining addition and scalar multiplication by

$$\begin{aligned}
(f_i) + (g_i) &= (f_i + g_i) \\
\lambda(f_i) &= (\lambda f_i).
\end{aligned}$$

The family $(e_i)_{i\in I}$ is defined such that $(e_i)_j = 0$ if $j \neq i$ and $(e_i)_i = 1$. It is a basis of the vector space $K^{(I)}$, so that every $w \in K^{(I)}$ can be uniquely written as a finite linear combination of the e_i. There is also an injection $\iota\colon I \to K^{(I)}$ such that $\iota(i) = e_i$ for every $i \in I$. Furthermore, it is easy to show that for any vector space F, and for any function

$h\colon I \to F$, there is a unique linear map $\overline{h}\colon K^{(I)} \to F$ such that $h = \overline{h} \circ \iota$, as in the following diagram.

$$\begin{tikzcd}
I \arrow[r, "\iota"] \arrow[dr, "h"'] & K^{(I)} \arrow[d, "\overline{h}"] \\
& F
\end{tikzcd}$$

Definition 33.5. The vector space $(K^{(I)}, \iota)$ constructed as above from a set I is called the *free vector space generated by* I (or over I). The commutativity of the above diagram is called the *universal mapping property* of the free vector space $(K^{(I)}, \iota)$ over I.

Using the proof technique of Proposition 33.5, it is not hard to prove that any two vector spaces satisfying the above universal mapping property are isomorphic.

We can now return to the construction of tensor products. For simplicity consider two vector spaces E_1 and E_2. Whatever $E_1 \otimes E_2$ and $\varphi\colon E_1 \times E_2 \to E_1 \otimes E_2$ are, since φ is supposed to be bilinear, we must have

$$\begin{aligned}
\varphi(u_1 + u_2, v_1) &= \varphi(u_1, v_1) + \varphi(u_2, v_1)\\
\varphi(u_1, v_1 + v_2) &= \varphi(u_1, v_1) + \varphi(u_1, v_2)\\
\varphi(\lambda u_1, v_1) &= \lambda\varphi(u_1, v_1)\\
\varphi(u_1, \mu v_1) &= \mu\varphi(u_1, v_1)
\end{aligned}$$

for all $u_1, u_2 \in E_1$, all $v_1, v_2 \in E_2$, and all $\lambda, \mu \in K$. Since $E_1 \otimes E_2$ must satisfy the universal mapping property of Definition 33.4, we may want to define $E_1 \otimes E_2$ as the free vector space $K^{(E_1 \times E_2)}$ generated by $I = E_1 \times E_2$ and let φ be the injection of $E_1 \times E_2$ into $K^{(E_1 \times E_2)}$. The problem is that in $K^{(E_1 \times E_2)}$, vectors such that

$$(u_1 + u_2, v_1) \quad \textit{and} \quad (u_1, v_1) + (u_2, v_2)$$

are different, when they should really be the same, since φ is bilinear. Since $K^{(E_1 \times E_2)}$ is free, there are no relations among the generators and this vector space is too big for our purpose.

The remedy is simple: take the quotient of the free vector space $K^{(E_1 \times E_2)}$ by the subspace N generated by the vectors of the form

$$\begin{aligned}
&(u_1 + u_2, v_1) - (u_1, v_1) - (u_2, v_1)\\
&(u_1, v_1 + v_2) - (u_1, v_1) - (u_1, v_2)\\
&(\lambda u_1, v_1) - \lambda(u_1, v_1)\\
&(u_1, \mu v_1) - \mu(u_1, v_1).
\end{aligned}$$

Then, if we let $E_1 \otimes E_2$ be the quotient space $K^{(E_1 \times E_2)}/N$ and let φ be the quotient map, this forces φ to be bilinear. Checking that $(K^{(E_1 \times E_2)}/N, \varphi)$ satisfies the universal mapping property is straightforward. Here is the detailed construction.

Theorem 33.6. *Given $n \geq 2$ vector spaces $E_1, \ldots, E_n$, a tensor product $(E_1 \otimes \cdots \otimes E_n, \varphi)$ for $E_1, \ldots, E_n$ can be constructed. Furthermore, denoting $\varphi(u_1, \ldots, u_n)$ as $u_1 \otimes \cdots \otimes u_n$, the tensor product $E_1 \otimes \cdots \otimes E_n$ is generated by the vectors $u_1 \otimes \cdots \otimes u_n$, where $u_1 \in E_1, \ldots, u_n \in E_n$, and for every multilinear map $f \colon E_1 \times \cdots \times E_n \to F$, the unique linear map $f_\otimes \colon E_1 \otimes \cdots \otimes E_n \to F$ such that $f = f_\otimes \circ \varphi$ is defined by*

$$f_\otimes(u_1 \otimes \cdots \otimes u_n) = f(u_1, \ldots, u_n)$$

on the generators $u_1 \otimes \cdots \otimes u_n$ of $E_1 \otimes \cdots \otimes E_n$.

Proof. First we apply the construction of a free vector space to the cartesian product $I = E_1 \times \cdots \times E_n$, obtaining the free vector space $M = K^{(I)}$ on $I = E_1 \times \cdots \times E_n$. Since every basis generator $e_i \in M$ is uniquely associated with some n-tuple $i = (u_1, \ldots, u_n) \in E_1 \times \cdots \times E_n$, we denote e_i by $(u_1, \ldots, u_n)$.

Next let N be the subspace of M generated by the vectors of the following type:

$$\begin{aligned}&(u_1, \ldots, u_i + v_i, \ldots, u_n) - (u_1, \ldots, u_i, \ldots, u_n) - (u_1, \ldots, v_i, \ldots, u_n),\\ &(u_1, \ldots, \lambda u_i, \ldots, u_n) - \lambda(u_1, \ldots, u_i, \ldots, u_n).\end{aligned}$$

We let $E_1 \otimes \cdots \otimes E_n$ be the quotient M/N of the free vector space M by N, $\pi \colon M \to M/N$ be the quotient map, and set

$$\varphi = \pi \circ \iota.$$

By construction, φ is multilinear, and since π is surjective and the $\iota(i) = e_i$ generate M, the fact that each i is of the form $i = (u_1, \ldots, u_n) \in E_1 \times \cdots \times E_n$ implies that $\varphi(u_1, \ldots, u_n)$ generate M/N. Thus, if we denote $\varphi(u_1, \ldots, u_n)$ as $u_1 \otimes \cdots \otimes u_n$, the space $E_1 \otimes \cdots \otimes E_n$ is generated by the vectors $u_1 \otimes \cdots \otimes u_n$, with $u_i \in E_i$.

It remains to show that $(E_1 \otimes \cdots \otimes E_n, \varphi)$ satisfies the universal mapping property. To this end, we begin by proving there is a map h such that $f = h \circ \varphi$. Since $M = K^{(E_1 \times \cdots \times E_n)}$ is free on $I = E_1 \times \cdots \times E_n$, there is a unique linear map $\overline{f} \colon K^{(E_1 \times \cdots \times E_n)} \to F$, such that

$$f = \overline{f} \circ \iota,$$

as in the diagram below.

$$\begin{tikzcd}
E_1 \times \cdots \times E_n \arrow[r, "\iota"] \arrow[dr, "f"'] & K^{(E_1 \times \cdots \times E_n)} = M \arrow[d, "\overline{f}"] \\
& F
\end{tikzcd}$$

Because f is multilinear, note that we must have $\overline{f}(w) = 0$ for every $w \in N$; for example, on the generator

$$(u_1, \ldots, u_i + v_i, \ldots, u_n) - (u_1, \ldots, u_i, \ldots, u_n) - (u_1, \ldots, v_i, \ldots, u_n)$$

we have

$$\begin{aligned}
&\overline{f}((u_1,\ldots,u_i+v_i,\ldots,u_n)-(u_1,\ldots,u_i,\ldots,u_n)-(u_1,\ldots,v_i,\ldots,u_n))\\
&\qquad = f(u_1,\ldots,u_i+v_i,\ldots,u_n)-f(u_1,\ldots,u_i,\ldots,u_n)-f(u_1,\ldots,v_i,\ldots,u_n)\\
&\qquad = f(u_1,\ldots,u_i,\ldots,u_n)+f(u_1,\ldots,v_i,\ldots,u_n)-f(u_1,\ldots,u_i,\ldots,u_n)\\
&\qquad\quad - f(u_1,\ldots,v_i,\ldots,u_n)\\
&\qquad = 0.
\end{aligned}$$

But then, $\overline{f}\colon M\to F$ factors through M/N, which means that there is a unique linear map $h\colon M/N\to F$ such that $\overline{f}=h\circ\pi$ making the following diagram commute

$$\begin{tikzcd}
M \arrow[r, "\pi"] \arrow[dr, "\overline{f}"'] & M/N \arrow[d, "h"] \\
 & F,
\end{tikzcd}$$

by defining $h([z])=\overline{f}(z)$ for every $z\in M$, where $[z]$ denotes the equivalence class in M/N of $z\in M$. Indeed, the fact that $\overline{f}$ vanishes on N insures that h is well defined on M/N, and it is clearly linear by definition. Since $f=\overline{f}\circ\iota$, from the equation $\overline{f}=h\circ\pi$, by composing on the right with ι, we obtain

$$f=\overline{f}\circ\iota=h\circ\pi\circ\iota=h\circ\varphi,$$

as in the following commutative diagram.

$$\begin{tikzcd}
 & K^{(E_1\times\cdots\times E_n)} \arrow[dd, "\overline{f}"] \arrow[dr, "\pi"] & \\
E_1\times\cdots\times E_n \arrow[ur, "\iota"] \arrow[dr, "f"'] & & K^{(E_1\times\cdots\times E_n)}/N \arrow[dl, "h"] \\
 & F &
\end{tikzcd}$$

We now prove the uniqueness of h. For any linear map $f_\otimes\colon E_1\otimes\cdots\otimes E_n\to F$ such that $f=f_\otimes\circ\varphi$, since the vectors $u_1\otimes\cdots\otimes u_n$ generate $E_1\otimes\cdots\otimes E_n$ and since $\varphi(u_1,\ldots,u_n)=u_1\otimes\cdots\otimes u_n$, the map $f_\otimes$ is uniquely defined by

$$f_\otimes(u_1\otimes\cdots\otimes u_n)=f(u_1,\ldots,u_n).$$

Since $f=h\circ\varphi$, the map h is unique, and we let $f_\otimes=h$. □

The map φ from $E_1\times\cdots\times E_n$ to $E_1\otimes\cdots\otimes E_n$ is often denoted by $\iota_\otimes$, so that

$$\iota_\otimes(u_1,\ldots,u_n)=u_1\otimes\cdots\otimes u_n.$$

What is important about Theorem 33.6 is not so much the construction itself but the fact that it produces a tensor product with the universal mapping property with respect to multilinear maps. Indeed, Theorem 33.6 yields a canonical isomorphism

$$\mathrm{L}(E_1 \otimes \cdots \otimes E_n, F) \cong \mathrm{L}(E_1, \ldots, E_n; F)$$

between the vector space of linear maps $\mathrm{L}(E_1 \otimes \cdots \otimes E_n, F)$, and the vector space of multilinear maps $\mathcal{L}(E_1, \ldots, E_n; F)$, *via* the linear map $- \circ \varphi$ defined by

$$h \mapsto h \circ \varphi,$$

where $h \in \mathrm{L}(E_1 \otimes \cdots \otimes E_n, F)$. Indeed, $h \circ \varphi$ is clearly multilinear, and since by Theorem 33.6, for every multilinear map $f \in \mathcal{L}(E_1, \ldots, E_n; F)$, there is a unique linear map $f_\otimes \in \mathrm{L}(E_1 \otimes \cdots \otimes E_n, F)$ such that $f = f_\otimes \circ \varphi$, the map $- \circ \varphi$ is bijective. As a matter of fact, its inverse is the map

$$f \mapsto f_\otimes.$$

We record this fact as the following proposition.

Proposition 33.7. *Given a tensor product $(E_1 \otimes \cdots \otimes E_n, \varphi)$, the linear map $h \mapsto h \circ \varphi$ is a canonical isomorphism*

$$\mathrm{L}(E_1 \otimes \cdots \otimes E_n, F) \cong \mathrm{L}(E_1, \ldots, E_n; F)$$

between the vector space of linear maps $\mathrm{L}(E_1 \otimes \cdots \otimes E_n, F)$, and the vector space of multilinear maps $\mathcal{L}(E_1, \ldots, E_n; F)$.

Using the "Hom" notation, the above canonical isomorphism is written

$$\mathrm{Hom}(E_1 \otimes \cdots \otimes E_n, F) \cong \mathrm{Hom}(E_1, \ldots, E_n; F).$$

Remarks:

(1) To be very precise, since the tensor product depends on the field K, we should subscript the symbol $\otimes$ with K and write

$$E_1 \otimes_K \cdots \otimes_K E_n.$$

However, we often omit the subscript K unless confusion may arise.

(2) For $F = K$, the base field, Proposition 33.7 yields a canonical isomorphism between the vector space $\mathrm{L}(E_1 \otimes \cdots \otimes E_n, K)$, and the vector space of multilinear forms $\mathcal{L}(E_1, \ldots, E_n; K)$. However, $\mathrm{L}(E_1 \otimes \cdots \otimes E_n, K)$ is the dual space $(E_1 \otimes \cdots \otimes E_n)^*$, and thus the vector space of multilinear forms $\mathcal{L}(E_1, \ldots, E_n; K)$ is canonically isomorphic to $(E_1 \otimes \cdots \otimes E_n)^*$.

Since this isomorphism is used often, we record it as the following proposition.

Proposition 33.8. *Given a tensor product $E_1 \otimes \cdots \otimes E_n$,, there is a canonical isomorphism*

$$\mathrm{L}(E_1, \ldots, E_n; K) \cong (E_1 \otimes \cdots \otimes E_n)^*$$

between the vector space of multilinear maps $\mathcal{L}(E_1, \ldots, E_n; K)$ and the dual $(E_1 \otimes \cdots \otimes E_n)^*$ of the tensor product $E_1 \otimes \cdots \otimes E_n$.

The fact that the map $\varphi\colon E_1 \times \cdots \times E_n \to E_1 \otimes \cdots \otimes E_n$ is multilinear, can also be expressed as follows:

$$\begin{aligned} u_1 \otimes \cdots \otimes (v_i + w_i) \otimes \cdots \otimes u_n &= (u_1 \otimes \cdots \otimes v_i \otimes \cdots \otimes u_n) + (u_1 \otimes \cdots \otimes w_i \otimes \cdots \otimes u_n), \\ u_1 \otimes \cdots \otimes (\lambda u_i) \otimes \cdots \otimes u_n &= \lambda (u_1 \otimes \cdots \otimes u_i \otimes \cdots \otimes u_n). \end{aligned}$$

Of course, this is just what we wanted!

Definition 33.6. Tensors in $E_1 \otimes \cdots \otimes E_n$ are called *n-tensors*, and tensors of the form $u_1 \otimes \cdots \otimes u_n$, where $u_i \in E_i$ are called *simple (or decomposable) n-tensors*. Those n-tensors that are not simple are often called *compound n-tensors*.

Not only do tensor products act on spaces, but they also act on linear maps (they are functors).

Proposition 33.9. *Given two linear maps $f\colon E \to E'$ and $g\colon F \to F'$, there is a unique linear map*

$$f \otimes g\colon E \otimes F \to E' \otimes F'$$

such that

$$(f \otimes g)(u \otimes v) = f(u) \otimes g(v),$$

for all $u \in E$ and all $v \in F$.

Proof. We can define $h\colon E \times F \to E' \otimes F'$ by

$$h(u, v) = f(u) \otimes g(v).$$

It is immediately verified that h is bilinear, and thus it induces a unique linear map

$$f \otimes g\colon E \otimes F \to E' \otimes F'$$

making the following diagram commutes

$$\begin{tikzcd} E \times F \arrow[r, "\iota_\otimes"] \arrow[dr, "h"'] & E \otimes F \arrow[d, "f \otimes g"] \\ & E' \otimes F', \end{tikzcd}$$

such that $(f \otimes g)(u \otimes v) = f(u) \otimes g(v)$, for all $u \in E$ and all $v \in F$. □

Definition 33.7. The linear map $f \otimes g \colon E \otimes F \to E' \otimes F'$ given by Proposition 33.9 is called the *tensor product* of $f \colon E \to E'$ and $g \colon F \to F'$.

Another way to define $f \otimes g$ proceeds as follows. Given two linear maps $f \colon E \to E'$ and $g \colon F \to F'$, the map $f \times g$ is the linear map from $E \times F$ to $E' \times F'$ given by

$$(f \times g)(u, v) = (f(u), g(v)), \quad \text{for all } u \in E \text{ and all } v \in F.$$

Then the map h in the proof of Proposition 33.9 is given by $h = \iota'_{\otimes} \circ (f \times g)$, and $f \otimes g$ is the unique linear map making the following diagram commute.

$$\begin{tikzcd}
E \times F \arrow[r, "\iota_{\otimes}"] \arrow[d, "f \times g"'] & E \otimes F \arrow[d, "f \otimes g"] \\
E' \times F' \arrow[r, "\iota'_{\otimes}"'] & E' \otimes F'
\end{tikzcd}$$

Remark: The notation $f \otimes g$ is potentially ambiguous, because $\mathrm{Hom}(E, F)$ and $\mathrm{Hom}(E', F')$ are vector spaces, so we can form the tensor product $\mathrm{Hom}(E, F) \otimes \mathrm{Hom}(E', F')$ which contains elements also denoted $f \otimes g$. To avoid confusion, the first kind of tensor product of linear maps defined in Proposition 33.9 (which yields a linear map in $\mathrm{Hom}(E \otimes F, E' \otimes F')$) can be denoted by $T(f, g)$. If we denote the tensor product $E \otimes F$ by $T(E, F)$, this notation makes it clearer that T is a bifunctor. If E, E' and F, F' are finite dimensional, by picking bases it is not hard to show that the map induced by $f \otimes g \mapsto T(f, g)$ is an isomorphism

$$\mathrm{Hom}(E, F) \otimes \mathrm{Hom}(E', F') \cong \mathrm{Hom}(E \otimes F, E' \otimes F').$$

Proposition 33.10. *Suppose we have linear maps $f \colon E \to E'$, $g \colon F \to F'$, $f' \colon E' \to E''$ and $g' \colon F' \to F''$. Then the following identity holds:*

$$(f' \circ f) \otimes (g' \circ g) = (f' \otimes g') \circ (f \otimes g). \tag{$*$}$$

Proof. We have the commutative diagram

$$\begin{tikzcd}
E \times F \arrow[r, "\iota_{\otimes}"] \arrow[d, "f \times g"'] & E \otimes F \arrow[d, "f \otimes g"] \\
E' \times F' \arrow[r, "\iota'_{\otimes}"] \arrow[d, "f' \times g'"'] & E' \otimes F' \arrow[d, "f' \otimes g'"] \\
E'' \times F'' \arrow[r, "\iota''_{\otimes}"'] & E'' \otimes F'',
\end{tikzcd}$$

and thus the commutative diagram.

$$\begin{tikzcd}
E \times F \arrow[r, "\iota_{\otimes}"] \arrow[d, "(f' \times g') \circ (f \times g)"'] & E \otimes F \arrow[d, "(f' \otimes g') \circ (f \otimes g)"] \\
E'' \times F'' \arrow[r, "\iota''_{\otimes}"'] & E'' \otimes F''
\end{tikzcd}$$

We also have the commutative diagram.

$$\begin{tikzcd}
E \times F \arrow[r, "\iota_\otimes"] \arrow[d, "(f'\circ f)\times(g'\circ g)"'] & E \otimes F \arrow[d, "(f'\circ f)\otimes(g'\circ g)"] \\
E'' \times F'' \arrow[r, "\iota''_\otimes"'] & E'' \otimes F''.
\end{tikzcd}$$

Since we immediately verify that

$$(f' \circ f) \times (g' \circ g) = (f' \times g') \circ (f \times g),$$

by uniqueness of the map between $E \otimes F$ and $E'' \otimes F''$ in the above diagram, we conclude that

$$(f' \circ f) \otimes (g' \circ g) = (f' \otimes g') \circ (f \otimes g),$$

as claimed. □

The above formula $(*)$ yields the following useful fact.

Proposition 33.11. *If $f\colon E \to E'$ and $g\colon F \to F'$ are isomorphims, then $f \otimes g\colon E \otimes F \to E' \otimes F'$ is also an isomorphism.*

Proof. If $f^{-1}\colon E' \to E$ is the inverse of $f\colon E \to E'$ and $g^{-1}\colon F' \to F$ is the inverse of $g\colon F \to F'$, then $f^{-1} \otimes g^{-1}\colon E' \otimes F' \to E \otimes F$ is the inverse of $f \otimes g\colon E \otimes F \to E' \otimes F'$, which is shown as follows:

$$\begin{aligned}
(f \otimes g) \circ (f^{-1} \otimes g^{-1}) &= (f \circ f^{-1}) \otimes (g \circ g^{-1}) \\
&= \mathrm{id}_{E'} \otimes \mathrm{id}_{F'} \\
&= \mathrm{id}_{E' \otimes F'},
\end{aligned}$$

and

$$\begin{aligned}
(f^{-1} \otimes g^{-1}) \circ (f \otimes g) &= (f^{-1} \circ f) \otimes (g^{-1} \circ g) \\
&= \mathrm{id}_{E} \otimes \mathrm{id}_{F} \\
&= \mathrm{id}_{E \otimes F}.
\end{aligned}$$

Therefore, $f \otimes g\colon E \otimes F \to E' \otimes F'$ is an isomorphism. □

The generalization to the tensor product $f_1 \otimes \cdots \otimes f_n$ of $n \geq 3$ linear maps $f_i\colon E_i \to F_i$ is immediate, and left to the reader.

33.3 Bases of Tensor Products

We showed that $E_1 \otimes \cdots \otimes E_n$ is generated by the vectors of the form $u_1 \otimes \cdots \otimes u_n$. However, these vectors are not linearly independent. This situation can be fixed when considering bases.

To explain the idea of the proof, consider the case when we have two spaces E and F both of dimension 3. Given a basis (e_1, e_2, e_3) of E and a basis (f_1, f_2, f_3) of F, we would like to prove that

$$e_1 \otimes f_1, \quad e_1 \otimes f_2, \quad e_1 \otimes f_3, \quad e_2 \otimes f_1, \quad e_2 \otimes f_2, \quad e_2 \otimes f_3, \quad e_3 \otimes f_1, \quad e_3 \otimes f_2, \quad e_3 \otimes f_3$$

are linearly independent. To prove this, it suffices to show that for any vector space G, if $w_{11}, w_{12}, w_{13}, w_{21}, w_{22}, w_{23}, w_{31}, w_{32}, w_{33}$ are any vectors in G, then there is a bilinear map $h\colon E \times F \to G$ such that

$$h(e_i, e_j) = w_{ij}, \quad 1 \leq i, j \leq 3.$$

Because h yields a unique linear map $h_\otimes\colon E \otimes F \to G$ such that

$$h_\otimes(e_i \otimes e_j) = w_{ij}, \quad 1 \leq i, j \leq 3,$$

and by Proposition 33.4, the vectors

$$e_1 \otimes f_1, \quad e_1 \otimes f_2, \quad e_1 \otimes f_3, \quad e_2 \otimes f_1, \quad e_2 \otimes f_2, \quad e_2 \otimes f_3, \quad e_3 \otimes f_1, \quad e_3 \otimes f_2, \quad e_3 \otimes f_3$$

are linearly independent. This suggests understanding how a bilinear function $f\colon E \times F \to G$ is expressed in terms of its values $f(e_i, f_j)$ on the basis vectors (e_1, e_2, e_3) and (f_1, f_2, f_3), and this can be done easily. Using bilinearity we obtain

$$\begin{aligned} f(u_1e_1 + u_2e_2 + u_3e_3, v_1f_1 + v_2f_2 + v_3f_3) &= u_1v_1f(e_1, f_1) + u_1v_2f(e_1, f_2) + u_1v_3f(e_1, f_3) \\ &\quad + u_2v_1f(e_2, f_1) + u_2v_2f(e_2, f_2) + u_2v_3f(e_2, f_3) \\ &\quad + u_3v_1f(e_3, f_1) + u_3v_2f(e_3, f_2) + u_3v_3f(e_3, f_3). \end{aligned}$$

Therefore, given $w_{11}, w_{12}, w_{13}, w_{21}, w_{22}, w_{23}, w_{31}, w_{32}, w_{33} \in G$, the function h given by

$$\begin{aligned} h(u_1e_1 + u_2e_2 + u_3e_3, v_1f_1 + v_2f_2 + v_3f_3) &= u_1v_1w_{11} + u_1v_2w_{12} + u_1v_3w_{13} \\ &\quad + u_2v_1w_{21} + u_2v_2w_{22} + u_2v_3w_{23} \\ &\quad + u_3v_1w_{31} + u_3v_2w_{33} + u_3v_3w_{33} \end{aligned}$$

is clearly bilinear, and by construction $h(e_i, f_j) = w_{ij}$, so it does the job.

The generalization of this argument to any number of vector spaces of any dimension (even infinite) is straightforward.

Proposition 33.12. *Given $n \geq 2$ vector spaces $E_1, \ldots, E_n$, if $(u_i^k)_{i \in I_k}$ is a basis for E_k, $1 \leq k \leq n$, then the family of vectors*

$$(u_{i_1}^1 \otimes \cdots \otimes u_{i_n}^n)_{(i_1, \ldots, i_n) \in I_1 \times \ldots \times I_n}$$

is a basis of the tensor product $E_1 \otimes \cdots \otimes E_n$.

Proof. For each k, $1 \leq k \leq n$, every $v^k \in E_k$ can be written uniquely as

$$v^k = \sum_{j \in I_k} v_j^k u_j^k,$$

for some family of scalars $(v_j^k)_{j \in I_k}$. Let F be any nontrivial vector space. We show that for every family

$$(w_{i_1,\ldots,i_n})_{(i_1,\ldots,i_n) \in I_1 \times \ldots \times I_n},$$

of vectors in F, there is some linear map $h\colon E_1 \otimes \cdots \otimes E_n \to F$ such that

$$h(u_{i_1}^1 \otimes \cdots \otimes u_{i_n}^n) = w_{i_1,\ldots,i_n}.$$

Then by Proposition 33.4, it follows that

$$(u_{i_1}^1 \otimes \cdots \otimes u_{i_n}^n)_{(i_1,\ldots,i_n) \in I_1 \times \ldots \times I_n}$$

is linearly independent. However, since $(u_i^k)_{i \in I_k}$ is a basis for E_k, the $u_{i_1}^1 \otimes \cdots \otimes u_{i_n}^n$ also generate $E_1 \otimes \cdots \otimes E_n$, and thus, they form a basis of $E_1 \otimes \cdots \otimes E_n$.

We define the function $f\colon E_1 \times \cdots \times E_n \to F$ as follows: For any n nonempty finite subsets $J_1, \ldots, J_n$ such that $J_k \subseteq I_k$ for $k = 1, \ldots, n$,

$$f(\sum_{j_1 \in J_1} v_{j_1}^1 u_{j_1}^1, \ldots, \sum_{j_n \in J_n} v_{j_n}^n u_{j_n}^n) = \sum_{j_1 \in J_1, \ldots, j_n \in J_n} v_{j_1}^1 \cdots v_{j_n}^n \, w_{j_1,\ldots,j_n}.$$

It is immediately verified that f is multilinear. By the universal mapping property of the tensor product, the linear map $f_\otimes\colon E_1 \otimes \cdots \otimes E_n \to F$ such that $f = f_\otimes \circ \varphi$, is the desired map h. □

In particular, when each I_k is finite and of size $m_k = \dim(E_k)$, we see that the dimension of the tensor product $E_1 \otimes \cdots \otimes E_n$ is $m_1 \cdots m_n$. As a corollary of Proposition 33.12, if $(u_i^k)_{i \in I_k}$ is a basis for E_k, $1 \leq k \leq n$, then every tensor $z \in E_1 \otimes \cdots \otimes E_n$ can be written in a unique way as

$$z = \sum_{(i_1,\ldots,i_n) \, \in \, I_1 \times \ldots \times I_n} \lambda_{i_1,\ldots,i_n} \, u_{i_1}^1 \otimes \cdots \otimes u_{i_n}^n,$$

for some unique family of scalars $\lambda_{i_1,\ldots,i_n} \in K$, all zero except for a finite number.

33.4 Some Useful Isomorphisms for Tensor Products

Proposition 33.13. *Given three vector spaces E, F, G, there exists unique canonical isomorphisms*

(1) $E \otimes F \cong F \otimes E$

(2) $(E \otimes F) \otimes G \cong E \otimes (F \otimes G) \cong E \otimes F \otimes G$

(3) $(E \oplus F) \otimes G \cong (E \otimes G) \oplus (F \otimes G)$

(4) $K \otimes E \cong E$

such that respectively

(a) $u \otimes v \mapsto v \otimes u$

(b) $(u \otimes v) \otimes w \mapsto u \otimes (v \otimes w) \mapsto u \otimes v \otimes w$

(c) $(u, v) \otimes w \mapsto (u \otimes w, v \otimes w)$

(d) $\lambda \otimes u \mapsto \lambda u$*.*

Proof. Except for (3), these isomorphisms are proved using the universal mapping property of tensor products.

(1) The map from $E \times F$ to $F \otimes E$ given by $(u, v) \mapsto v \otimes u$ is clearly bilinear, thus it induces a unique linear $\alpha\colon E \otimes F \to F \otimes E$ making the following diagram commute

$$\begin{tikzcd} E \times F \arrow[r, "\iota_\otimes"] \arrow[dr] & E \otimes F \arrow[d, "\alpha"] \\ & F \otimes E, \end{tikzcd}$$

such that

$$\alpha(u \otimes v) = v \otimes u, \quad \text{for all } u \in E \text{ and all } v \in F.$$

Similarly, the map from $F \times E$ to $E \otimes F$ given by $(v, u) \mapsto u \otimes v$ is clearly bilinear, thus it induces a unique linear $\beta\colon F \otimes E \to E \otimes F$ making the following diagram commute

$$\begin{tikzcd} F \times E \arrow[r, "\iota_\otimes"] \arrow[dr] & F \otimes E \arrow[d, "\beta"] \\ & E \otimes F, \end{tikzcd}$$

such that

$$\beta(v \otimes u) = u \otimes v, \quad \text{for all } u \in E \text{ and all } v \in F.$$

It is immediately verified that

$$(\beta \circ \alpha)(u \otimes v) = u \otimes v \quad \text{and} \quad (\alpha \circ \beta)(v \otimes u) = v \otimes u$$

for all $u \in E$ and all $v \in F$. Since the tensors of the form $u \otimes v$ span $E \otimes F$ and similarly the tensors of the form $v \otimes u$ span $F \otimes E$, the map $\beta \circ \alpha$ is actually the identity on $E \otimes F$, and similarly $\alpha \circ \beta$ is the identity on $F \otimes E$, so α and β are isomorphisms.

(2) Fix some $w \in G$. The map

$$(u, v) \mapsto u \otimes v \otimes w$$

from $E \times F$ to $E \otimes F \otimes G$ is bilinear, and thus there is a linear map $f_w \colon E \otimes F \to E \otimes F \otimes G$ making the following diagram commute

$$\begin{tikzcd}
E \times F \arrow[r, "\iota_\otimes"] \arrow[dr] & E \otimes F \arrow[d, "f_w"] \\
 & E \otimes F \otimes G,
\end{tikzcd}$$

with $f_w(u \otimes v) = u \otimes v \otimes w$.

Next consider the map

$$(z, w) \mapsto f_w(z),$$

from $(E \otimes F) \times G$ into $E \otimes F \otimes G$. It is easily seen to be bilinear, and thus it induces a linear map $f \colon (E \otimes F) \otimes G \to E \otimes F \otimes G$ making the following diagram commute

$$\begin{tikzcd}
(E \otimes F) \times G \arrow[r, "\iota_\otimes"] \arrow[dr] & (E \otimes F) \otimes G \arrow[d, "f"] \\
 & E \otimes F \otimes G,
\end{tikzcd}$$

with $f((u \otimes v) \otimes w) = u \otimes v \otimes w$.

Also consider the map

$$(u, v, w) \mapsto (u \otimes v) \otimes w$$

from $E \times F \times G$ to $(E \otimes F) \otimes G$. It is trilinear, and thus there is a linear map $g \colon E \otimes F \otimes G \to (E \otimes F) \otimes G$ making the following diagram commute

$$\begin{tikzcd}
E \times F \times G \arrow[r, "\iota_\otimes"] \arrow[dr] & E \otimes F \otimes G \arrow[d, "g"] \\
 & (E \otimes F) \otimes G,
\end{tikzcd}$$

with $g(u \otimes v \otimes w) = (u \otimes v) \otimes w$. Clearly, $f \circ g$ and $g \circ f$ are identity maps, and thus f and g are isomorphisms. The other case is similar.

(3) Given a fixed vector space G, for any two vector spaces M and N and every linear map $f \colon M \to N$, let $\tau_G(f) = f \otimes \mathrm{id}_G$ be the unique linear map making the following diagram commute.

$$\begin{tikzcd}
M \times G \arrow[r, "\iota_{M\otimes}"] \arrow[d, "f \times \mathrm{id}_G"'] & M \otimes G \arrow[d, "f \otimes \mathrm{id}_G"] \\
N \times G \arrow[r, "\iota_{N\otimes}"'] & N \otimes G
\end{tikzcd}$$

The identity $(*)$ proved in Proposition 33.10 shows that if $g\colon N \to P$ is another linear map, then

$$\tau_G(g) \circ \tau_G(f) = (g \otimes \mathrm{id}_G) \circ (f \otimes \mathrm{id}_G) = (g \circ f) \otimes (\mathrm{id}_G \circ \mathrm{id}_G) = (g \circ f) \otimes \mathrm{id}_G = \tau_G(g \circ f).$$

Clearly, $\tau_G(0) = 0$, and a direct computation on generators also shows that

$$\tau_G(\mathrm{id}_M) = (\mathrm{id}_M \otimes \mathrm{id}_G) = \mathrm{id}_{M\otimes G},$$

and that if $f'\colon M \to N$ is another linear map, then

$$\tau_G(f + f') = \tau_G(f) + \tau_G(f').$$

In fancy terms, τ_G is a functor. Now, if $E \oplus F$ is a direct sum, it is a standard fact of linear algebra that if $\pi_E\colon E \oplus F \to E$ and $\pi_F\colon E \oplus F \to F$ are the projection maps, then

$$\pi_E \circ \pi_E = \pi_E \qquad \pi_F \circ \pi_F = \pi_F \qquad \pi_E \circ \pi_F = 0 \qquad \pi_F \circ \pi_E = 0 \qquad \pi_E + \pi_F = \mathrm{id}_{E\oplus F}.$$

If we apply τ_G to these identites, we get

$$\begin{array}{lll} \tau_G(\pi_E) \circ \tau_G(\pi_E) = \tau_G(\pi_E) & \tau_G(\pi_F) \circ \tau_G(\pi_F) = \tau_G(\pi_F) & \\ \tau_G(\pi_E) \circ \tau_G(\pi_F) = 0 & \tau_G(\pi_F) \circ \tau_G(\pi_E) = 0 & \tau_G(\pi_E) + \tau_G(\pi_F) = \mathrm{id}_{(E\oplus F)\otimes G}. \end{array}$$

Observe that $\tau_G(\pi_E) = \pi_E \otimes \mathrm{id}_G$ is a map from $(E \oplus F) \otimes G$ onto $E \otimes G$ and that $\tau_G(\pi_F) = \pi_F \otimes \mathrm{id}_G$ is a map from $(E \oplus F) \otimes G$ onto $F \otimes G$, and by linear algebra, the above equations mean that we have a direct sum

$$(E \otimes G) \oplus (F \otimes G) \cong (E \oplus F) \otimes G.$$

(4) We have the linear map $\epsilon\colon E \to K \otimes E$ given by

$$\epsilon(u) = 1 \otimes u, \quad \text{for all } u \in E.$$

The map $(\lambda, u) \mapsto \lambda u$ from $K \times E$ to E is bilinear, so it induces a unique linear map $\eta\colon K \otimes E \to E$ making the following diagram commute

$$\begin{tikzcd} K \times E \arrow[r, "\iota_\otimes"] \arrow[dr] & K \otimes E \arrow[d, "\eta"] \\ & E, \end{tikzcd}$$

such that $\eta(\lambda \otimes u) = \lambda u$, for all $\lambda \in K$ and all $u \in E$. We have

$$(\eta \circ \epsilon)(u) = \eta(1 \otimes u) = 1u = u,$$

and

$$(\epsilon \circ \eta)(\lambda \otimes u) = \epsilon(\lambda u) = 1 \otimes (\lambda u) = \lambda(1 \otimes u) = \lambda \otimes u,$$

which shows that both $\epsilon \circ \eta$ and $\eta \circ \epsilon$ are the identity, so ϵ and η are isomorphisms. □

Remark: The isomorphism (3) can be generalized to finite and even arbitrary direct sums $\bigoplus_{i\in I} E_i$ of vector spaces (where I is an arbitrary nonempty index set). We have an isomorphism

$$\left(\bigoplus_{i\in I} E_i\right) \otimes G \cong \bigoplus_{i\in I} (E_i \otimes G).$$

This isomorphism (with isomorphism (1)) can be used to give another proof of Proposition 33.12 (see Bertin [15], Chapter 4, Section 1) or Lang [108], Chapter XVI, Section 2).

Proposition 33.14. *Given any three vector spaces E, F, G, we have the canonical isomorphism*

$$\mathrm{Hom}(E, F; G) \cong \mathrm{Hom}(E, \mathrm{Hom}(F, G)).$$

Proof. Any bilinear map $f\colon E \times F \to G$ gives the linear map $\varphi(f) \in \mathrm{Hom}(E, \mathrm{Hom}(F, G))$, where $\varphi(f)(u)$ is the linear map in $\mathrm{Hom}(F, G)$ given by

$$\varphi(f)(u)(v) = f(u, v).$$

Conversely, given a linear map $g \in \mathrm{Hom}(E, \mathrm{Hom}(F, G))$, we get the bilinear map $\psi(g)$ given by

$$\psi(g)(u, v) = g(u)(v),$$

and it is clear that φ and ψ and mutual inverses. □

Since by Proposition 33.7 there is a canonical isomorphism

$$\mathrm{Hom}(E \otimes F, G) \cong \mathrm{Hom}(E, F; G),$$

together with the isomorphism

$$\mathrm{Hom}(E, F; G) \cong \mathrm{Hom}(E, \mathrm{Hom}(F, G))$$

given by Proposition 33.14, we obtain the important corollary:

Proposition 33.15. *For any three vector spaces E, F, G, we have the canonical isomorphism*

$$\mathrm{Hom}(E \otimes F, G) \cong \mathrm{Hom}(E, \mathrm{Hom}(F, G)).$$

33.5 Duality for Tensor Products

In this section all vector spaces are assumed to have *finite dimension*, unless specified otherwise. Let us now see how tensor products behave under duality. For this, we define a pairing between $E_1^* \otimes \cdots \otimes E_n^*$ and $E_1 \otimes \cdots \otimes E_n$ as follows: For any fixed $(v_1^*, \ldots, v_n^*) \in E_1^* \times \cdots \times E_n^*$, we have the multilinear map

$$l_{v_1^*,\ldots,v_n^*}\colon (u_1, \ldots, u_n) \mapsto v_1^*(u_1) \cdots v_n^*(u_n)$$

from $E_1 \times \cdots \times E_n$ to K. The map $l_{v_1^*,\ldots,v_n^*}$ extends uniquely to a linear map $L_{v_1^*,\ldots,v_n^*}\colon E_1 \otimes \cdots \otimes E_n \longrightarrow K$ making the following diagram commute.

$$\begin{tikzcd}
E_1 \times \cdots \times E_n \arrow[r, "\iota_\otimes"] \arrow[dr, "l_{v_1^*,\ldots,v_n^*}"'] & E_1 \otimes \cdots \otimes E_n \arrow[d, "L_{v_1^*,\ldots,v_n^*}"] \\
 & K
\end{tikzcd}$$

We also have the multilinear map

$$(v_1^*, \ldots, v_n^*) \mapsto L_{v_1^*,\ldots,v_n^*}$$

from $E_1^* \times \cdots \times E_n^*$ to $\mathrm{Hom}(E_1 \otimes \cdots \otimes E_n, K)$, which extends to a unique linear map L from $E_1^* \otimes \cdots \otimes E_n^*$ to $\mathrm{Hom}(E_1 \otimes \cdots \otimes E_n, K)$ making the following diagram commute.

$$\begin{tikzcd}
E_1^* \times \cdots \times E_n^* \arrow[r, "\iota_\otimes"] \arrow[dr, "L_{v_1^*,\ldots,v_n^*}"'] & E_1^* \otimes \cdots \otimes E_n^* \arrow[d, "L"] \\
 & \mathrm{Hom}(E_1 \otimes \cdots \otimes E_n; K)
\end{tikzcd}$$

However, in view of the isomorphism

$$\mathrm{Hom}(U \otimes V, W) \cong \mathrm{Hom}(U, \mathrm{Hom}(V, W))$$

given by Proposition 33.15, with $U = E_1^* \otimes \cdots \otimes E_n^*$, $V = E_1 \otimes \cdots \otimes E_n$ and $W = K$, we can view L as a linear map

$$L\colon (E_1^* \otimes \cdots \otimes E_n^*) \otimes (E_1 \otimes \cdots \otimes E_n) \to K,$$

which corresponds to a bilinear map

$$\langle -, - \rangle\colon (E_1^* \otimes \cdots \otimes E_n^*) \times (E_1 \otimes \cdots \otimes E_n) \longrightarrow K, \tag{††}$$

via the isomorphism $(U \otimes V)^* \cong \mathrm{Hom}(U, V; K)$ given by Proposition 33.8. This pairing is given explicitly on generators by

$$\langle v_1^* \otimes \cdots \otimes v_n^*, u_1 \ldots, u_n \rangle = v_1^*(u_1) \cdots v_n^*(u_n).$$

This pairing is nondegenerate, as proved below.

Proof. If $(e_1^1, \ldots, e_{m_1}^1), \ldots, (e_1^n, \ldots, e_{m_n}^n)$ are bases for $E_1, \ldots, E_n$, then for every basis element $(e_{i_1}^1)^* \otimes \cdots \otimes (e_{i_n}^n)^*$ of $E_1^* \otimes \cdots \otimes E_n^*$, and any basis element $e_{j_1}^1 \otimes \cdots \otimes e_{j_n}^n$ of $E_1 \otimes \cdots \otimes E_n$, we have

$$\langle (e_{i_1}^1)^* \otimes \cdots \otimes (e_{i_n}^n)^*, e_{j_1}^1 \otimes \cdots \otimes e_{j_n}^n \rangle = \delta_{i_1\, j_1} \cdots \delta_{i_n\, j_n},$$

where $\delta_{i\,j}$ is *Kronecker delta*, defined such that $\delta_{i\,j} = 1$ if $i = j$, and 0 otherwise. Given any $\alpha \in E_1^* \otimes \cdots \otimes E_n^*$, assume that $\langle \alpha, \beta \rangle = 0$ for all $\beta \in E_1 \otimes \cdots \otimes E_n$. The vector α is a finite linear combination $\alpha = \sum \lambda_{i_1,\ldots,i_n} (e^1_{i_1})^* \otimes \cdots \otimes (e^n_{i_n})^*$, for some unique $\lambda_{i_1,\ldots,i_n} \in K$. If we choose $\beta = e^1_{i_1} \otimes \cdots \otimes e^n_{i_n}$, then we get

$$\begin{aligned} 0 = \langle \alpha, e^1_{i_1} \otimes \cdots \otimes e^n_{i_n} \rangle &= \left\langle \sum \lambda_{i_1,\ldots,i_n} (e^1_{i_1})^* \otimes \cdots \otimes (e^n_{i_n})^*, e^1_{i_1} \otimes \cdots \otimes e^n_{i_n} \right\rangle \\ &= \sum \lambda_{i_1,\ldots,i_n} \langle (e^1_{i_1})^* \otimes \cdots \otimes (e^n_{i_n})^*, e^1_{i_1} \otimes \cdots \otimes e^n_{i_n} \rangle \\ &= \lambda_{i_1,\ldots,i_n}. \end{aligned}$$

Therefore, $\alpha = 0$,

Conversely, given any $\beta \in E_1 \otimes \cdots \otimes E_n$, assume that $\langle \alpha, \beta \rangle = 0$, for all $\alpha \in E_1^* \otimes \cdots \otimes E_n^*$. The vector β is a finite linear combination $\beta = \sum \lambda_{i_1,\ldots,i_n} e^1_{i_1} \otimes \cdots \otimes e^n_{i_n}$, for some unique $\lambda_{i_1,\ldots,i_n} \in K$. If we choose $\alpha = (e^1_{i_1})^* \otimes \cdots \otimes (e^n_{i_n})^*$, then we get

$$\begin{aligned} 0 = \langle (e^1_{i_1})^* \otimes \cdots \otimes (e^n_{i_n})^*, \beta \rangle &= \left\langle (e^1_{i_1})^* \otimes \cdots \otimes (e^n_{i_n})^*, \sum \lambda_{i_1,\ldots,i_n} e^1_{i_1} \otimes \cdots \otimes e^n_{i_n} \right\rangle \\ &= \sum \lambda_{i_1,\ldots,i_n} \langle (e^1_{i_1})^* \otimes \cdots \otimes (e^n_{i_n})^*, e^1_{i_1} \otimes \cdots \otimes e^n_{i_n} \rangle \\ &= \lambda_{i_1,\ldots,i_n}. \end{aligned}$$

Therefore, $\beta = 0$. □

By Proposition 33.1,[1] we have a canonical isomorphism

$$(E_1 \otimes \cdots \otimes E_n)^* \cong E_1^* \otimes \cdots \otimes E_n^*.$$

Here is our main proposition about duality of tensor products.

Proposition 33.16. *We have canonical isomorphisms*

$$(E_1 \otimes \cdots \otimes E_n)^* \cong E_1^* \otimes \cdots \otimes E_n^*,$$

and

$$\mu \colon E_1^* \otimes \cdots \otimes E_n^* \cong \mathrm{Hom}(E_1, \ldots, E_n; K).$$

Proof. The second isomorphism follows from the isomorphism $(E_1 \otimes \cdots \otimes E_n)^* \cong E_1^* \otimes \cdots \otimes E_n^*$ together with the isomorphism $\mathrm{Hom}(E_1, \ldots, E_n; K) \cong (E_1 \otimes \cdots \otimes E_n)^*$ given by Proposition 33.8. □

Remarks:

1. The isomorphism $\mu \colon E_1^* \otimes \cdots \otimes E_n^* \cong \mathrm{Hom}(E_1, \ldots, E_n; K)$ can be described explicitly as the linear extension to $E_1^* \otimes \cdots \otimes E_n^*$ of the map given by

$$\mu(v_1^* \otimes \cdots \otimes v_n^*)(u_1 \ldots, u_n) = v_1^*(u_1) \cdots v_n^*(u_n).$$

[1] This is where the assumption that our spaces are finite-dimensional is used.

2. The canonical isomorphism of Proposition 33.16 holds under more general conditions. Namely, that K is a commutative ring with identity and that the E_i are finitely-generated projective K-modules (see Definition 35.7). See Bourbaki, [25] (Chapter III, §11, Section 5, Proposition 7).

We prove another useful canonical isomorphism that allows us to treat linear maps as tensors.

Let E and F be two vector spaces and let $\alpha\colon E^* \times F \to \mathrm{Hom}(E, F)$ be the map defined such that

$$\alpha(u^*, f)(x) = u^*(x)f,$$

for all $u^* \in E^*$, $f \in F$, and $x \in E$. This map is clearly bilinear, and thus it induces a linear map $\alpha_\otimes\colon E^* \otimes F \to \mathrm{Hom}(E, F)$ making the following diagram commute

$$\begin{tikzcd}
E^* \times F \arrow[r, "\iota_\otimes"] \arrow[dr, "\alpha"'] & E^* \otimes F \arrow[d, "\alpha_\otimes"] \\
& \mathrm{Hom}(E, F),
\end{tikzcd}$$

such that

$$\alpha_\otimes(u^* \otimes f)(x) = u^*(x)f.$$

Proposition 33.17. *If E and F are vector spaces (not necessarily finite dimensional), then the following properties hold:*

(1) The linear map $\alpha_\otimes\colon E^* \otimes F \to \mathrm{Hom}(E, F)$ is injective.

(2) If E is finite-dimensional, then $\alpha_\otimes\colon E^* \otimes F \to \mathrm{Hom}(E, F)$ is a canonical isomorphism.

(3) If F is finite-dimensional, then $\alpha_\otimes\colon E^* \otimes F \to \mathrm{Hom}(E, F)$ is a canonical isomorphism.

Proof. (1) Let $(e_i^*)_{i\in I}$ be a basis of E^* and let $(f_j)_{j\in J}$ be a basis of F. Then we know that $(e_i^* \otimes f_j)_{i\in I, j\in J}$ is a basis of $E^* \otimes F$. To prove that $\alpha_\otimes$ is injective, let us show that its kernel is reduced to (0). For any vector

$$\omega = \sum_{i\in I', j\in J'} \lambda_{ij}\, e_i^* \otimes f_j$$

in $E^* \otimes F$, with I' and J' some finite sets, assume that $\alpha_\otimes(\omega) = 0$. This means that for every $x \in E$, we have $\alpha_\otimes(\omega)(x) = 0$; that is,

$$\sum_{i\in I', j\in J'} \alpha_\otimes(\lambda_{ij}\, e_i^* \otimes f_j)(x) = \sum_{j\in J'} \Biggl(\sum_{i\in I'} \lambda_{ij} e_i^*(x)\Biggr) f_j = 0.$$

Since $(f_j)_{j\in J}$ is a basis of F, for every $j \in J'$, we must have

$$\sum_{i\in I'} \lambda_{ij} e_i^*(x) = 0, \quad \text{for all } x \in E.$$

But then $(e_i^*)_{i\in I'}$ would be linearly dependent, contradicting the fact that $(e_i^*)_{i\in I}$ is a basis of E^*, so we must have

$$\lambda_{ij} = 0, \quad \text{for all } i \in I' \text{ and all } j \in J',$$

which shows that $\omega = 0$. Therefore, $\alpha_\otimes$ is injective.

(2) Let $(e_j)_{1\leq j\leq n}$ be a finite basis of E, and as usual, let $e_j^* \in E^*$ be the linear form defined by

$$e_j^*(e_k) = \delta_{j,k},$$

where $\delta_{j,k} = 1$ iff $j = k$ and 0 otherwise. We know that $(e_j^*)_{1\leq j\leq n}$ is a basis of E^* (this is where we use the finite dimension of E). For any linear map $f \in \mathrm{Hom}(E, F)$, for every $x = x_1e_1 + \cdots + x_ne_n \in E$, we have

$$f(x) = f(x_1e_1 + \cdots + x_ne_n) = x_1f(e_1) + \cdots + x_nf(e_n) = e_1^*(x)f(e_1) + \cdots + e_n^*(x)f(e_n).$$

Consequently, every linear map $f \in \mathrm{Hom}(E, F)$ can be expressed as

$$f(x) = e_1^*(x)f_1 + \cdots + e_n^*(x)f_n,$$

for some $f_i \in F$. Furthermore, if we apply f to e_i, we get $f(e_i) = f_i$, so the f_i are unique. Observe that

$$(\alpha_\otimes(e_1^* \otimes f_1 + \cdots + e_n^* \otimes f_n))(x) = \sum_{i=1}^n (\alpha_\otimes(e_i^* \otimes f_i))(x) = \sum_{i=1}^n e_i^*(x)f_i.$$

Thus, $\alpha_\otimes$ is surjective, so $\alpha_\otimes$ is a bijection.

(3) Let $(f_1, \ldots, f_m)$ be a finite basis of F, and let $(f_1^*, \ldots, f_m^*)$ be its dual basis. Given any linear map $h\colon E \to F$, for all $u \in E$, since $f_i^*(f_j) = \delta_{ij}$, we have

$$h(u) = \sum_{i=1}^m f_i^*(h(u))f_i.$$

If

$$h(u) = \sum_{j=1}^m v_j^*(u)f_j \quad \text{for all } u \in E \tag{$*$}$$

for some linear forms $(v_1^*, \ldots, v_m^*) \in (E^*)^m$, then

$$f_i^*(h(u)) = \sum_{j=1}^m v_j^*(u)f_i^*(f_j) = v_i^*(u) \quad \text{for all } u \in E,$$

which shows that $v_i^* = f_i^* \circ h$ for $i = 1, \ldots, m$. This means that h has a unique expression in terms of linear forms as in $(*)$. Define the map α from $(E^*)^m$ to $\mathrm{Hom}(E, F)$ by

$$\alpha(v_1^*, \ldots, v_m^*)(u) = \sum_{j=1}^{m} v_j^*(u) f_j \quad \text{for all } u \in E.$$

This map is linear. For any $h \in \mathrm{Hom}(E, F)$, we showed earlier that the expression of h in $(*)$ is unique, thus α is an isomorphism. Similarly, $E^* \otimes F$ is isomorphic to $(E^*)^m$. Any tensor $\omega \in E^* \otimes F$ can be written as a linear combination

$$\sum_{k=1}^{p} u_k^* \otimes y_k$$

for some $u_k^* \in E^*$ and some $y_k \in F$, and since $(f_1, \ldots, f_m)$ is a basis of F, each y_k can be written as a linear combination of $(f_1, \ldots, f_m)$, so ω can be expressed as

$$\omega = \sum_{i=1}^{m} v_i^* \otimes f_i, \tag{$\dagger$}$$

for some linear forms $v_i^* \in E^*$ which are linear combinations of the u_k^*. If we pick a basis $(w_i^*)_{i \in I}$ for E^*, then we know that the family $(w_i^* \otimes f_j)_{i \in I, 1 \leq j \leq m}$ is a basis of $E^* \otimes F$, and this implies that the v_i^* in $(\dagger)$ are unique. Define the linear map β from $(E^*)^m$ to $E^* \otimes F$ by

$$\beta(v_1^*, \ldots, v_m^*) = \sum_{i=1}^{m} v_i^* \otimes f_i.$$

Since every tensor $\omega \in E^* \otimes F$ can be written in a unique way as in $(\dagger)$, this map is an isomorphism. □

Note that in Proposition 33.17, we have an isomorphism if either E or F has finite dimension. The following proposition allows us to view a multilinear as a tensor product.

Proposition 33.18. *If the $E_1, \ldots E_n$ are finite-dimensional vector spaces and F is any vector space, then we have the canonical isomorphism*

$$\mathrm{Hom}(E_1, \ldots, E_n; F) \cong E_1^* \otimes \cdots \otimes E_n^* \otimes F.$$

Proof. In view of the canonical isomorphism

$$\mathrm{Hom}(E_1, \ldots, E_n; F) \cong \mathrm{Hom}(E_1 \otimes \cdots \otimes E_n, F)$$

given by Proposition 33.7 and the canonical isomorphism $(E_1 \otimes \cdots \otimes E_n)^* \cong E_1^* \otimes \cdots \otimes E_n^*$ given by Proposition 33.16, if the E_i's are finite-dimensional, then Proposition 33.17 yields the canonical isomorphism

$$\mathrm{Hom}(E_1, \ldots, E_n; F) \cong E_1^* \otimes \cdots \otimes E_n^* \otimes F,$$

as claimed. □

33.6 Tensor Algebras

Our goal is to define a vector space $T(V)$ obtained by taking the direct sum of the tensor products

$$\underbrace{V \otimes \cdots \otimes V}_{m},$$

and to define a multiplication operation on $T(V)$ which makes $T(V)$ into an algebraic structure called an algebra. The algebra $T(V)$ satisfies a universal property stated in Proposition 33.19, which makes it the "free algebra" generated by the vector space V.

Definition 33.8. The tensor product

$$\underbrace{V \otimes \cdots \otimes V}_{m}$$

is also denoted as

$$\bigotimes^m V \quad \text{or} \quad V^{\otimes m}$$

and is called the *m-th tensor power of* V (with $V^{\otimes 1} = V$, and $V^{\otimes 0} = K$).

We can pack all the tensor powers of V into the "big" vector space

$$T(V) = \bigoplus_{m \geq 0} V^{\otimes m},$$

denoted $T^{\bullet}(V)$ or $\bigotimes V$ to avoid confusion with the tangent bundle.

This is an interesting object because we can define a multiplication operation on it which makes it into an *algebra*.

When V is of finite dimension n, we can pick some basis $(e_1 \ldots, e_n)$ of V, and then every tensor $\omega \in T(V)$ can be expressed as a linear combination of terms of the form $e_{i_1} \otimes \cdots \otimes e_{i_k}$, where $(i_1, \ldots, i_k)$ is any sequence of elements from the set $\{1, \ldots, n\}$. We can think of the tensors $e_{i_1} \otimes \cdots \otimes e_{i_k}$ as monomials in the noncommuting variables $e_1, \ldots, e_n$. Thus the space $T(V)$ corresponds to the algebra of polynomials with coefficients in K in n *noncommuting variables.*

Let us review the definition of an algebra over a field. Let K denote any (commutative) field, although for our purposes, we may assume that $K = \mathbb{R}$ (and occasionally, $K = \mathbb{C}$). Since we will only be dealing with associative algebras with a multiplicative unit, we only define algebras of this kind.

Definition 33.9. Given a field K, a *K-algebra* is a K-vector space A together with a bilinear operation $\cdot \colon A \times A \to A$, called *multiplication*, which makes A into a ring with unity 1 (or 1_A, when we want to be very precise). This means that $\cdot$ is associative and that there is a multiplicative identity element 1 so that $1 \cdot a = a \cdot 1 = a$, for all $a \in A$. Given two

K-algebras A and B, a *K-algebra homomorphism* $h\colon A \to B$ is a linear map that is also a ring homomorphism, with $h(1_A) = 1_B$; that is,

$$\begin{aligned} h(a_1 \cdot a_2) &= h(a_1) \cdot h(a_2) \quad \text{for all } a_1, a_2 \in A \\ h(1_A) &= 1_B. \end{aligned}$$

The set of K-algebra homomorphisms between A and B is denoted $\mathrm{Hom}_{\mathrm{alg}}(A, B)$.

For example, the ring $\mathrm{M}_n(K)$ of all $n \times n$ matrices over a field K is a K-algebra.

There is an obvious notion of ideal of a K-algebra.

Definition 33.10. Let A be a K-algebra. An *ideal* $\mathfrak{A} \subseteq A$ is a linear subspace of A that is also a two-sided ideal with respect to multiplication in A; this means that for all $a \in \mathfrak{A}$ and all $\alpha, \beta \in A$, we have $\alpha a \beta \in \mathfrak{A}$.

If the field K is understood, we usually simply say an algebra instead of a K-algebra.

We would like to define a multiplication operation on $T(V)$ which makes it into a K-algebra. As

$$T(V) = \bigoplus_{i \geq 0} V^{\otimes i},$$

for every $i \geq 0$, there is a natural injection $\iota_n\colon V^{\otimes n} \to T(V)$, and in particular, an injection $\iota_0\colon K \to T(V)$. The multiplicative unit $\mathbf{1}$ of $T(V)$ is the image $\iota_0(1)$ in $T(V)$ of the unit 1 of the field K. Since every $v \in T(V)$ can be expressed as a finite sum

$$v = \iota_{n_1}(v_1) + \cdots + \iota_{n_k}(v_k),$$

where $v_i \in V^{\otimes n_i}$ and the n_i are natural numbers with $n_i \neq n_j$ if $i \neq j$, to define multiplication in $T(V)$, using bilinearity, it is enough to define multiplication operations $\cdot\colon V^{\otimes m} \times V^{\otimes n} \longrightarrow V^{\otimes (m+n)}$, which, using the isomorphisms $V^{\otimes n} \cong \iota_n(V^{\otimes n})$, yield multiplication operations $\cdot\colon \iota_m(V^{\otimes m}) \times \iota_n(V^{\otimes n}) \longrightarrow \iota_{m+n}(V^{\otimes (m+n)})$. First, for $\omega_1 \in V^{\otimes m}$ and $\omega_2 \in V^{\otimes n}$, we let

$$\omega_1 \cdot \omega_2 = \omega_1 \otimes \omega_2.$$

This defines a bilinear map so it defines a multiplication $V^{\otimes m} \times V^{\otimes n} \longrightarrow V^{\otimes m} \otimes V^{\otimes n}$. This is not quite what we want, but there is a canonical isomorphism

$$V^{\otimes m} \otimes V^{\otimes n} \cong V^{\otimes (m+n)}$$

which yields the desired multiplication $\cdot\colon V^{\otimes m} \times V^{\otimes n} \longrightarrow V^{\otimes (m+n)}$.

The isomorphism $V^{\otimes m} \otimes V^{\otimes n} \cong V^{\otimes (m+n)}$ can be established by induction using the isomorphism $(E \otimes F) \otimes G \cong E \otimes F \otimes G$. First we prove by induction on $m \geq 2$ that

$$V^{\otimes (m-1)} \otimes V \cong V^{\otimes m},$$

and then by induction on $n \geq 1$ than

$$V^{\otimes m} \otimes V^{\otimes n} \cong V^{\otimes(m+n)}.$$

In summary the multiplication $V^{\otimes m} \times V^{\otimes n} \longrightarrow V^{\otimes(m+n)}$ is defined so that

$$(v_1 \otimes \cdots \otimes v_m) \cdot (w_1 \otimes \cdots \otimes w_n) = v_1 \otimes \cdots \otimes v_m \otimes w_1 \otimes \cdots \otimes w_n.$$

(This has to be made rigorous by using isomorphisms involving the associativity of tensor products, for details, see Jacobson [96], Section 3.9, or Bertin [15], Chapter 4, Section 2.)

Definition 33.11. Given a K-vector space V (not necessarily finite dimensional), the vector space

$$T(V) = \bigoplus_{m \geq 0} V^{\otimes m}$$

denoted $T^{\bullet}(V)$ or $\bigotimes V$ equipped with the multiplication operations $V^{\otimes m} \times V^{\otimes n} \longrightarrow V^{\otimes(m+n)}$ defined above is called the *tensor algebra of* V.

Remark: It is important to note that multiplication in $T(V)$ is **not** commutative. Also, in all rigor, the unit $\mathbf{1}$ of $T(V)$ is **not equal** to 1, the unit of the field K. However, in view of the injection $\iota_0 \colon K \to T(V)$, for the sake of notational simplicity, we will denote $\mathbf{1}$ by 1. More generally, in view of the injections $\iota_n \colon V^{\otimes n} \to T(V)$, we identify elements of $V^{\otimes n}$ with their images in $T(V)$.

The algebra $T(V)$ satisfies a universal mapping property which shows that it is unique up to isomorphism. For simplicity of notation, let $i \colon V \to T(V)$ be the natural injection of V into $T(V)$.

Proposition 33.19. *Given any K-algebra A, for any linear map $f \colon V \to A$, there is a unique K-algebra homomorphism $\overline{f} \colon T(V) \to A$ so that*

$$f = \overline{f} \circ i,$$

as in the diagram below.

$$\begin{tikzcd}
V \arrow[r, "i"] \arrow[dr, "f"'] & T(V) \arrow[d, "\overline{f}"] \\
& A
\end{tikzcd}$$

Proof. Left an an exercise (use Theorem 33.6). A proof can be found in Knapp [103] (Appendix A, Proposition A.14) or Bertin [15] (Chapter 4, Theorem 2.4). □

Proposition 33.19 implies that there is a natural isomorphism

$$\mathrm{Hom}_{\mathrm{alg}}(T(V), A) \cong \mathrm{Hom}(V, A),$$

where the algebra A on the right-hand side is viewed as a vector space. Proposition 33.19 also has the following corollary.

Proposition 33.20. *Given a linear map $h\colon V_1 \to V_2$ between two vectors spaces V_1, V_2 over a field K, there is a unique K-algebra homomorphism $\otimes h\colon T(V_1) \to T(V_2)$ making the following diagram commute.*

$$\begin{tikzcd}
V_1 \arrow[r, "i_1"] \arrow[d, "h"'] & T(V_1) \arrow[d, "\otimes h"] \\
V_2 \arrow[r, "i_2"] & T(V_2).
\end{tikzcd}$$

Most algebras of interest arise as well-chosen quotients of the tensor algebra $T(V)$. This is true for the *exterior algebra* $\bigwedge(V)$ (also called *Grassmann algebra*), where we take the quotient of $T(V)$ modulo the ideal generated by all elements of the form $v \otimes v$, where $v \in V$,and for the *symmetric algebra* $\mathrm{Sym}(V)$, where we take the quotient of $T(V)$ modulo the ideal generated by all elements of the form $v \otimes w - w \otimes v$, where $v, w \in V$.

Algebras such as $T(V)$ are graded in the sense that there is a sequence of subspaces $V^{\otimes n} \subseteq T(V)$ such that

$$T(V) = \bigoplus_{k \geq 0} V^{\otimes n},$$

and the multiplication $\otimes$ behaves well w.r.t. the grading, *i.e.*, $\otimes\colon V^{\otimes m} \times V^{\otimes n} \to V^{\otimes(m+n)}$.

Definition 33.12. A K-algebra E is said to be a *graded algebra* iff there is a sequence of subspaces $E^n \subseteq E$ such that

$$E = \bigoplus_{k \geq 0} E^n,$$

(with $E^0 = K$) and the multiplication $\cdot$ respects the grading; that is, $\cdot\colon E^m \times E^n \to E^{m+n}$. Elements in E^n are called *homogeneous elements of rank (or degree) n.*

In differential geometry and in physics it is necessary to consider slightly more general tensors.

Definition 33.13. Given a vector space V, for any pair of nonnegative integers (r, s), the *tensor space $T^{r,s}(V)$ of type* (r, s) is the tensor product

$$T^{r,s}(V) = V^{\otimes r} \otimes (V^*)^{\otimes s} = \underbrace{V \otimes \cdots \otimes V}_{r} \otimes \underbrace{V^* \otimes \cdots \otimes V^*}_{s},$$

with $T^{0,0}(V) = K$. We also define the *tensor algebra* $T^{\bullet,\bullet}(V)$ as the direct sum (coproduct)

$$T^{\bullet,\bullet}(V) = \bigoplus_{r,s \geq 0} T^{r,s}(V).$$

Tensors in $T^{r,s}(V)$ are called *homogeneous of degree (r, s).*

Note that tensors in $T^{r,0}(V)$ are just our "old tensors" in $V^{\otimes r}$. We make $T^{\bullet,\bullet}(V)$ into an algebra by defining multiplication operations

$$T^{r_1,s_1}(V) \times T^{r_2,s_2}(V) \longrightarrow T^{r_1+r_2,s_1+s_2}(V)$$

in the usual way, namely: For $u = u_1 \otimes \cdots \otimes u_{r_1} \otimes u_1^* \otimes \cdots \otimes u_{s_1}^*$ and
$v = v_1 \otimes \cdots \otimes v_{r_2} \otimes v_1^* \otimes \cdots \otimes v_{s_2}^*$, let

$$u \otimes v = u_1 \otimes \cdots \otimes u_{r_1} \otimes v_1 \otimes \cdots \otimes v_{r_2} \otimes u_1^* \otimes \cdots \otimes u_{s_1}^* \otimes v_1^* \otimes \cdots \otimes v_{s_2}^*.$$

Denote by $\mathrm{Hom}(V^r, (V^*)^s; W)$ the vector space of all multilinear maps from $V^r \times (V^*)^s$ to W. Then we have the universal mapping property which asserts that there is a canonical isomorphism

$$\mathrm{Hom}(T^{r,s}(V), W) \cong \mathrm{Hom}(V^r, (V^*)^s; W).$$

In particular,

$$(T^{r,s}(V))^* \cong \mathrm{Hom}(V^r, (V^*)^s; K).$$

For finite dimensional vector spaces, the duality of Section 33.5 is also easily extended to the tensor spaces $T^{r,s}(V)$. We define the pairing

$$T^{r,s}(V^*) \times T^{r,s}(V) \longrightarrow K$$

as follows: if

$$v^* = v_1^* \otimes \cdots \otimes v_r^* \otimes u_{r+1} \otimes \cdots \otimes u_{r+s} \in T^{r,s}(V^*)$$

and

$$u = u_1 \otimes \cdots \otimes u_r \otimes v_{r+1}^* \otimes \cdots \otimes v_{r+s}^* \in T^{r,s}(V),$$

then

$$(v^*, u) = v_1^*(u_1) \cdots v_{r+s}^*(u_{r+s}).$$

This is a nondegenerate pairing, and thus we get a canonical isomorphism

$$(T^{r,s}(V))^* \cong T^{r,s}(V^*).$$

Consequently, we get a canonical isomorphism

$$T^{r,s}(V^*) \cong \mathrm{Hom}(V^r, (V^*)^s; K).$$

We summarize these results in the following proposition.

Proposition 33.21. *Let V be a vector space and let*

$$T^{r,s}(V) = V^{\otimes r} \otimes (V^*)^{\otimes s} = \underbrace{V \otimes \cdots \otimes V}_{r} \otimes \underbrace{V^* \otimes \cdots \otimes V^*}_{s}.$$

We have the canonical isomorphisms

$$(T^{r,s}(V))^* \cong T^{r,s}(V^*),$$

and

$$T^{r,s}(V^*) \cong \mathrm{Hom}(V^r, (V^*)^s; K).$$

Remark: The tensor spaces, $T^{r,s}(V)$ are also denoted $T^r_s(V)$. A tensor $\alpha \in T^{r,s}(V)$ is said to be *contravariant* in the first r arguments and *covariant* in the last s arguments. This terminology refers to the way tensors behave under coordinate changes. Given a basis $(e_1, \ldots, e_n)$ of V, if $(e_1^*, \ldots, e_n^*)$ denotes the dual basis, then every tensor $\alpha \in T^{r,s}(V)$ is given by an expression of the form

$$\alpha = \sum_{\substack{i_1,\ldots,i_r \\ j_1,\ldots,j_s}} a^{i_1,\ldots,i_r}_{j_1,\ldots,j_s} e_{i_1} \otimes \cdots \otimes e_{i_r} \otimes e^*_{j_1} \otimes \cdots \otimes e^*_{j_s}.$$

The tradition in classical tensor notation is to use lower indices on vectors and upper indices on linear forms and in accordance to *Einstein summation convention* (or *Einstein notation*) the position of the indices on the coefficients is reversed. *Einstein summation convention* (already encountered in Section 33.1) is to assume that a summation is performed for all values of every index that appears simultaneously once as an upper index and once as a lower index. According to this convention, the tensor α above is written

$$\alpha = a^{i_1,\ldots,i_r}_{j_1,\ldots,j_s} e_{i_1} \otimes \cdots \otimes e_{i_r} \otimes e^{j_1} \otimes \cdots \otimes e^{j_s}.$$

An older view of tensors is that they are multidimensional arrays of coefficients,

$$\left(a^{i_1,\ldots,i_r}_{j_1,\ldots,j_s}\right),$$

subject to the rules for changes of bases.

Another operation on general tensors, contraction, is useful in differential geometry.

Definition 33.14. For all $r, s \geq 1$, the *contraction* $c_{i,j}\colon T^{r,s}(V) \to T^{r-1,s-1}(V)$, with $1 \leq i \leq r$ and $1 \leq j \leq s$, is the linear map defined on generators by

$$\begin{aligned} & c_{i,j}(u_1 \otimes \cdots \otimes u_r \otimes v_1^* \otimes \cdots \otimes v_s^*) \\ & \qquad = \; v_j^*(u_i)\, u_1 \otimes \cdots \otimes \widehat{u_i} \otimes \cdots \otimes u_r \otimes v_1^* \otimes \cdots \otimes \widehat{v_j^*} \otimes \cdots \otimes v_s^*, \end{aligned}$$

where the hat over an argument means that it should be omitted.

Let us figure our what is $c_{1,1}\colon T^{1,1}(V) \to \mathbb{R}$, that is $c_{1,1}\colon V \otimes V^* \to \mathbb{R}$. If $(e_1, \ldots, e_n)$ is a basis of V and $(e_1^*, \ldots, e_n^*)$ is the dual basis, by Proposition 33.17 every $h \in V \otimes V^* \cong \mathrm{Hom}(V, V)$ can be expressed as

$$h = \sum_{i,j=1}^n a_{ij}\, e_i \otimes e_j^*.$$

As

$$c_{1,1}(e_i \otimes e_j^*) = \delta_{i,j},$$

we get

$$c_{1,1}(h) = \sum_{i=1}^n a_{ii} = \mathrm{tr}(h),$$

where $\mathrm{tr}(h)$ is the *trace* of h, where h is viewed as the linear map given by the matrix, (a_{ij}). Actually, since $c_{1,1}$ is defined independently of any basis, $c_{1,1}$ provides an intrinsic definition of the trace of a linear map $h \in \mathrm{Hom}(V, V)$.

Remark: Using the Einstein summation convention, if

$$\alpha = a^{i_1,\ldots,i_r}_{j_1,\ldots,j_s} e_{i_1} \otimes \cdots \otimes e_{i_r} \otimes e^{j_1} \otimes \cdots \otimes e^{j_s},$$

then

$$c_{k,l}(\alpha) = a^{i_1,\ldots,i_{k-1},i_{k+1}\ldots,i_r}_{j_1,\ldots,j_{l-1},j_{l+1},\ldots,j_s} e_{i_1} \otimes \cdots \otimes \widehat{e_{i_k}} \otimes \cdots \otimes e_{i_r} \otimes e^{j_1} \otimes \cdots \otimes \widehat{e^{j_l}} \otimes \cdots \otimes e^{j_s}.$$

If E and F are two K-algebras, we know that their tensor product $E \otimes F$ exists as a vector space. We can make $E \otimes F$ into an algebra as well. Indeed, we have the multilinear map

$$E \times F \times E \times F \longrightarrow E \otimes F$$

given by $(a, b, c, d) \mapsto (ac) \otimes (bd)$, where ac is the product of a and c in E and bd is the product of b and d in F. By the universal mapping property, we get a linear map,

$$E \otimes F \otimes E \otimes F \longrightarrow E \otimes F.$$

Using the isomorphism

$$E \otimes F \otimes E \otimes F \cong (E \otimes F) \otimes (E \otimes F),$$

we get a linear map

$$(E \otimes F) \otimes (E \otimes F) \longrightarrow E \otimes F,$$

and thus a bilinear map,

$$(E \otimes F) \times (E \otimes F) \longrightarrow E \otimes F$$

which is our multiplication operation in $E \otimes F$. This multiplication is determined by

$$(a \otimes b) \cdot (c \otimes d) = (ac) \otimes (bd).$$

In summary we have the following proposition.

Proposition 33.22. *Given two K-algebra E and F, the operation on $E \otimes F$ defined on generators by*

$$(a \otimes b) \cdot (c \otimes d) = (ac) \otimes (bd)$$

makes $E \otimes F$ into a K-algebra.

We now turn to symmetric tensors.

33.7 Symmetric Tensor Powers

Our goal is to come up with a notion of tensor product that will allow us to treat symmetric multilinear maps as linear maps. Note that we have to restrict ourselves to a *single* vector space E, rather then n vector spaces $E_1, \ldots, E_n$, so that symmetry makes sense.

Definition 33.15. A multilinear map $f\colon E^n \to F$ is *symmetric* iff

$$f(u_{\sigma(1)}, \ldots, u_{\sigma(n)}) = f(u_1, \ldots, u_n),$$

for all $u_i \in E$ and all permutations, $\sigma\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$. The group of permutations on $\{1, \ldots, n\}$ (the *symmetric group*) is denoted $\mathfrak{S}_n$. The vector space of all symmetric multilinear maps $f\colon E^n \to F$ is denoted by $\mathrm{Sym}^n(E; F)$ or $\mathrm{Hom}_{\mathrm{symlin}}(E^n, F)$. Note that $\mathrm{Sym}^1(E; F) = \mathrm{Hom}(E, F)$.

We could proceed directly as in Theorem 33.6 and construct symmetric tensor products from scratch. However, since we already have the notion of a tensor product, there is a more economical method. First we define symmetric tensor powers.

Definition 33.16. An *n-th symmetric tensor power* of a vector space E, where $n \geq 1$, is a vector space S together with a symmetric multilinear map $\varphi\colon E^n \to S$ such that, for every vector space F and for every symmetric multilinear map $f\colon E^n \to F$, there is a unique linear map $f_\odot\colon S \to F$, with

$$f(u_1, \ldots, u_n) = f_\odot(\varphi(u_1, \ldots, u_n)),$$

for all $u_1, \ldots, u_n \in E$, or for short

$$f = f_\odot \circ \varphi.$$

Equivalently, there is a unique linear map $f_\odot$ such that the following diagram commutes.

$$\begin{tikzcd}
E^n \arrow[r, "\varphi"] \arrow[rd, "f"'] & S \arrow[d, "f_\odot"] \\
 & F
\end{tikzcd}$$

The above property is called the *universal mapping property* of the symmetric tensor power (S, φ).

We next show that any two symmetric n-th tensor powers (S_1, φ_1) and (S_2, φ_2) for E are isomorphic.

Proposition 33.23. *Given any two symmetric n-th tensor powers (S_1, φ_1) and (S_2, φ_2) for E, there is an isomorphism $h\colon S_1 \to S_2$ such that*

$$\varphi_2 = h \circ \varphi_1.$$

Proof. Replace tensor product by n-th symmetric tensor power in the proof of Proposition 33.5. □

We now give a construction that produces a symmetric n-th tensor power of a vector space E.

Theorem 33.24. *Given a vector space E, a symmetric n-th tensor power $(\mathrm{S}^n(E), \varphi)$ for E can be constructed ($n \geq 1$). Furthermore, denoting $\varphi(u_1, \ldots, u_n)$ as $u_1 \odot \cdots \odot u_n$, the symmetric tensor power $\mathrm{S}^n(E)$ is generated by the vectors $u_1 \odot \cdots \odot u_n$, where $u_1, \ldots, u_n \in E$, and for every symmetric multilinear map $f\colon E^n \to F$, the unique linear map $f_\odot\colon \mathrm{S}^n(E) \to F$ such that $f = f_\odot \circ \varphi$ is defined by*

$$f_\odot(u_1 \odot \cdots \odot u_n) = f(u_1, \ldots, u_n)$$

on the generators $u_1 \odot \cdots \odot u_n$ of $\mathrm{S}^n(E)$.

Proof. The tensor power $E^{\otimes n}$ is too big, and thus we define an appropriate quotient. Let C be the subspace of $E^{\otimes n}$ generated by the vectors of the form

$$u_1 \otimes \cdots \otimes u_n - u_{\sigma(1)} \otimes \cdots \otimes u_{\sigma(n)},$$

for all $u_i \in E$, and all permutations $\sigma\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$. We claim that the quotient space $(E^{\otimes n})/C$ does the job.

Let $p\colon E^{\otimes n} \to (E^{\otimes n})/C$ be the quotient map, and let $\varphi\colon E^n \to (E^{\otimes n})/C$ be the map given by

$$\varphi = p \circ \varphi_0,$$

where $\varphi_0\colon E^n \to E^{\otimes n}$ is the injection given by $\varphi_0(u_1, \ldots, u_n) = u_1 \otimes \cdots \otimes u_n$.

Let us denote $\varphi(u_1, \ldots, u_n)$ as $u_1 \odot \cdots \odot u_n$. It is clear that φ is symmetric. Since the vectors $u_1 \otimes \cdots \otimes u_n$ generate $E^{\otimes n}$, and p is surjective, the vectors $u_1 \odot \cdots \odot u_n$ generate $(E^{\otimes n})/C$.

It remains to show that $((E^{\otimes n})/C, \varphi)$ satisfies the universal mapping property. To this end we begin by proving that there is a map h such that $f = h \circ \varphi$. Given any symmetric multilinear map $f\colon E^n \to F$, by Theorem 33.6 there is a linear map $f_\otimes\colon E^{\otimes n} \to F$ such that $f = f_\otimes \circ \varphi_0$, as in the diagram below.

$$\begin{tikzcd}
E^n \arrow[r, "\varphi_0"] \arrow[dr, "f"'] & E^{\otimes n} \arrow[d, "f_\otimes"] \\
& F
\end{tikzcd}$$

However, since f is symmetric, we have $f_{\otimes}(z) = 0$ for every $z \in C$. Thus, we get an induced linear map $h\colon (E^{\otimes n})/C \to F$ making the following diagram commute.

$$\begin{tikzcd}
 & E^{\otimes n} \arrow[dr, "p"] \arrow[dd, "f_{\otimes}"] & \\
E^n \arrow[ur, "\varphi_0"] \arrow[dr, "f"'] & & (E^{\otimes n})/C \arrow[dl, "h"] \\
 & F &
\end{tikzcd}$$

If we define $h([z]) = f_{\otimes}(z)$ for every $z \in E^{\otimes n}$, where $[z]$ is the equivalence class in $(E^{\otimes n})/C$ of $z \in E^{\otimes n}$, the above diagram shows that $f = h \circ p \circ \varphi_0 = h \circ \varphi$. We now prove the uniqueness of h. For any linear map $f_{\odot}\colon (E^{\otimes n})/C \to F$ such that $f = f_{\odot} \circ \varphi$, since $\varphi(u_1, \ldots, u_n) = u_1 \odot \cdots \odot u_n$ and the vectors $u_1 \odot \cdots \odot u_n$ generate $(E^{\otimes n})/C$, the map $f_{\odot}$ is uniquely defined by

$$f_{\odot}(u_1 \odot \cdots \odot u_n) = f(u_1, \ldots, u_n).$$

Since $f = h \circ \varphi$, the map h is unique, and we let $f_{\odot} = h$. Thus, $\mathrm{S}^n(E) = (E^{\otimes n})/C$ and φ constitute a symmetric n-th tensor power of E. □

The map φ from E^n to $\mathrm{S}^n(E)$ is often denoted $\iota_{\odot}$, so that

$$\iota_{\odot}(u_1, \ldots, u_n) = u_1 \odot \cdots \odot u_n.$$

Again, the actual construction is not important. What is important is that the symmetric n-th power has the universal mapping property with respect to symmetric multilinear maps.

Remark: The notation $\odot$ for the commutative multiplication of symmetric tensor powers is not standard. Another notation commonly used is $\cdot$. We often abbreviate "symmetric tensor power" as "symmetric power." The symmetric power $\mathrm{S}^n(E)$ is also denoted $\mathrm{Sym}^n E$ but we prefer to use the notation Sym to denote spaces of symmetric multilinear maps. To be consistent with the use of $\odot$, we could have used the notation $\bigodot^n E$. Clearly, $\mathrm{S}^1(E) \cong E$ and it is convenient to set $\mathrm{S}^0(E) = K$.

The fact that the map $\varphi\colon E^n \to \mathrm{S}^n(E)$ is symmetric and multilinear can also be expressed as follows:

$$\begin{aligned}
u_1 \odot \cdots \odot (v_i + w_i) \odot \cdots \odot u_n &= (u_1 \odot \cdots \odot v_i \odot \cdots \odot u_n) + (u_1 \odot \cdots \odot w_i \odot \cdots \odot u_n),\\
u_1 \odot \cdots \odot (\lambda u_i) \odot \cdots \odot u_n &= \lambda(u_1 \odot \cdots \odot u_i \odot \cdots \odot u_n),\\
u_{\sigma(1)} \odot \cdots \odot u_{\sigma(n)} &= u_1 \odot \cdots \odot u_n,
\end{aligned}$$

for all permutations $\sigma \in \mathfrak{S}_n$.

The last identity shows that the "operation" $\odot$ is commutative. This allows us to view the symmetric tensor $u_1 \odot \cdots \odot u_n$ as an object called a multiset.

Given a set A, a multiset with elements from A is a generalization of the concept of a set that allows multiple instances of elements from A to occur. For example, if $A = \{a, b, c, d\}$, the following are multisets:

$$M_1 = \{a, a, b\}, \;\; M_2 = \{a, a, b, b, c\}, \;\; M_3 = \{a, a, b, b, c, d, d, d\}.$$

Here is another way to represent multisets as tables showing the multiplicities of the elements in the multiset:

$$M_1 = \begin{pmatrix} a & b & c & d \\ 2 & 1 & 0 & 0 \end{pmatrix}, \quad M_2 = \begin{pmatrix} a & b & c & d \\ 2 & 2 & 1 & 0 \end{pmatrix}, \quad M_3 = \begin{pmatrix} a & b & c & d \\ 2 & 2 & 1 & 3 \end{pmatrix}.$$

The above are just graphs of functions from the set $A = \{a, b, c, d\}$ to $\mathbb{N}$. This suggests the following definition.

Definition 33.17. A finite *multiset* M over a set A is a function $M \colon A \to \mathbb{N}$ such that $M(a) \neq 0$ for finitely many $a \in A$. The *multiplicity* of an element $a \in A$ in M is $M(a)$. The set of all multisets over A is denoted by $\mathbb{N}^{(A)}$, and we let $\mathrm{dom}(M) = \{a \in A \mid M(a) \neq 0\}$, which is a finite set. The set $\mathrm{dom}(M)$ is the set of elements in A that actually occur in M. For any multiset $M \in \mathbb{N}^{(A)}$, note that $\sum_{a \in A} M(a)$ makes sense, since $\sum_{a \in A} M(a) = \sum_{a \in \mathrm{dom}(A)} M(a)$, and $\mathrm{dom}(M)$ is finite; this sum is the total number of elements in the multiset A and is called the *size* of M. Let $|M| = \sum_{a \in A} M(a)$.

Going back to our symmetric tensors, we can view the tensors of the form $u_1 \odot \cdots \odot u_n$ as multisets of size n over the set E.

Theorem 33.24 implies the following proposition.

Proposition 33.25. *There is a canonical isomorphism*

$$\mathrm{Hom}(\mathrm{S}^n(E), F) \cong \mathrm{Sym}^n(E; F),$$

between the vector space of linear maps $\mathrm{Hom}(\mathrm{S}^n(E), F)$ *and the vector space of symmetric multilinear maps* $\mathrm{Sym}^n(E; F)$ *given by the linear map* $- \circ \varphi$ *defined by* $h \mapsto h \circ \varphi$*, with* $h \in \mathrm{Hom}(\mathrm{S}^n(E), F)$*.*

Proof. The map $h \circ \varphi$ is clearly symmetric multilinear. By Theorem 33.24, for every symmetric multilinear map $f \in \mathrm{Sym}^n(E; F)$ there is a unique linear map $f_\odot \in \mathrm{Hom}(\mathrm{S}^n(E), F)$ such that $f = f_\odot \circ \varphi$, so the map $- \circ \varphi$ is bijective. Its inverse is the map $f \mapsto f_\odot$. □

In particular, when $F = K$, we get the following important fact.

Proposition 33.26. *There is a canonical isomorphism*

$$(\mathrm{S}^n(E))^* \cong \mathrm{Sym}^n(E; K).$$

Definition 33.18. Symmetric tensors in $\mathrm{S}^n(E)$ are called *symmetric n-tensors*, and tensors of the form $u_1 \odot \cdots \odot u_n$, where $u_i \in E$, are called *simple (or decomposable) symmetric n-tensors*. Those symmetric n-tensors that are not simple are often called *compound symmetric n-tensors*.

Given two linear maps $f\colon E \to E'$ and $g\colon E \to E'$, since the map $\iota'_\odot \circ (f \times g)$ is bilinear and symmetric, there is a unique linear map $f \odot g\colon \mathrm{S}^2(E) \to \mathrm{S}^2(E)'$ making the following diagram commute.

$$\begin{tikzcd}
E^2 \arrow[r, "\iota_\odot"] \arrow[d, "f\times g"'] & \mathrm{S}^2(E) \arrow[d, "f\odot g"] \\
(E')^2 \arrow[r, "\iota'_\odot"'] & \mathrm{S}^2(E').
\end{tikzcd}$$

Observe that $f \odot g$ is determined by

$$(f \odot g)(u \odot v) = f(u) \odot g(u).$$

Proposition 33.27. *Given any linear maps $f\colon E \to E'$, $g\colon E \to E'$, $f'\colon E' \to E''$, and $g'\colon E' \to E''$, we have*

$$(f' \circ f) \odot (g' \circ g) = (f' \odot g') \circ (f \odot g).$$

The generalization to the symmetric tensor product $f_1 \odot \cdots \odot f_n$ of $n \geq 3$ linear maps $f_i\colon E \to E'$ is immediate, and left to the reader.

33.8 Bases of Symmetric Powers

The vectors $u_1 \odot \cdots \odot u_m$ where $u_1, \ldots, u_m \in E$ generate $\mathrm{S}^m(E)$, but they are not linearly independent. We will prove a version of Proposition 33.12 for symmetric tensor powers using multisets.

Recall that a (finite) multiset over a set I is a function $M\colon I \to \mathbb{N}$, such that $M(i) \neq 0$ for finitely many $i \in I$. The set of all multisets over I is denoted as $\mathbb{N}^{(I)}$ and we let $\mathrm{dom}(M) = \{i \in I \mid M(i) \neq 0\}$, the finite set of elements in I that actually occur in M. The size of the multiset M is $|M| = \sum_{a \in A} M(a)$.

To explain the idea of the proof, consider the case when $m = 2$ and E has dimension 3. Given a basis (e_1, e_2, e_3) of E, we would like to prove that

$$e_1 \odot e_1, \quad e_1 \odot e_2, \quad e_1 \odot e_3, \quad e_2 \odot e_2, \quad e_2 \odot e_3, \quad e_3 \odot e_3$$

are linearly independent. To prove this, it suffices to show that for any vector space F, if $w_{11}, w_{12}, w_{13}, w_{22}, w_{23}, w_{33}$ are any vectors in F, then there is a symmetric bilinear map $h\colon E^2 \to F$ such that

$$h(e_i, e_j) = w_{ij}, \quad 1 \leq i \leq j \leq 3.$$

Because h yields a unique linear map $h_{\odot}\colon \mathrm{S}^2(E) \to F$ such that

$$h_{\odot}(e_i \odot e_j) = w_{ij}, \quad 1 \leq i \leq j \leq 3,$$

by Proposition 33.4, the vectors

$$e_1 \odot e_1, \quad e_1 \odot e_2, \quad e_1 \odot e_3, \quad e_2 \odot e_2, \quad e_2 \odot e_3, \quad e_3 \odot e_3$$

are linearly independent. This suggests understanding how a symmetric bilinear function $f\colon E^2 \to F$ is expressed in terms of its values $f(e_i, e_j)$ on the basis vectors (e_1, e_2, e_3), and this can be done easily. Using bilinearity and symmetry, we obtain

$$\begin{aligned} f(u_1e_1 + u_2e_2 + u_3e_3, v_1e_1 + v_2e_2 + v_3e_3) &= u_1v_1f(e_1, e_1) + (u_1v_2 + u_2v_1)f(e_1, e_2) \\ &\quad + (u_1v_3 + u_3v_1)f(e_1, e_3) + u_2v_2f(e_2, e_2) \\ &\quad + (u_2v_3 + u_3v_2)f(e_2, e_3) + u_3v_3f(e_3, e_3). \end{aligned}$$

Therefore, given $w_{11}, w_{12}, w_{13}, w_{22}, w_{23}, w_{33} \in F$, the function h given by

$$\begin{aligned} h(u_1e_1 + u_2e_2 + u_3e_3, v_1e_1 + v_2e_2 + v_3e_3) &= u_1v_1w_{11} + (u_1v_2 + u_2v_1)w_{12} \\ &\quad + (u_1v_3 + u_3v_1)w_{13} + u_2v_2w_{22} \\ &\quad + (u_2v_3 + u_3v_2)w_{23} + u_3v_3w_{33} \end{aligned}$$

is clearly bilinear symmetric, and by construction $h(e_i, e_j) = w_{ij}$, so it does the job.

The generalization of this argument to any $m \geq 2$ and to a space E of any dimension (even infinite) is conceptually clear, but notationally messy. If $\dim(E) = n$ and if $(e_1, \ldots, e_n)$ is a basis of E, for any m vectors $v_j = \sum_{i=1}^n u_{i,j}e_i$ in E, for any symmetric multilinear map $f\colon E^m \to F$, we have

$$\begin{aligned} & f(v_1, \ldots, v_m) \\ &= \sum_{k_1+\cdots+k_n=m} \left(\sum_{\substack{I_1\cup\cdots\cup I_n=\{1,\ldots,m\} \\ I_i\cap I_j=\emptyset,\, i\neq j,\, |I_j|=k_j}} \left(\prod_{i_1\in I_1} u_{1,i_1} \right) \cdots \left(\prod_{i_n\in I_n} u_{n,i_n} \right) \right) f(\underbrace{e_1, \ldots, e_1}_{k_1}, \ldots, \underbrace{e_n, \ldots, e_n}_{k_n}). \end{aligned}$$

Definition 33.19. Given any set J of $n \geq 1$ elements, say $J = \{j_1, \ldots, j_n\}$, and given any $m \geq 2$, for any sequence $(k_1 \ldots, k_n)$ of natural numbers $k_i \in \mathbb{N}$ such that $k_1 + \cdots + k_n = m$, the multiset M of size m

$$M = \{\underbrace{j_1, \ldots, j_1}_{k_1}, \underbrace{j_2, \ldots, j_2}_{k_2}, \ldots, \underbrace{j_n, \ldots, j_n}_{k_n}\}$$

is denoted by $M(m, J, k_1, \ldots, k_n)$. Note that $M(j_i) = k_i$, for $i = 1, \ldots, n$. Given any $k \geq 1$, and any $u \in E$, we denote $\underbrace{u \odot \cdots \odot u}_{k}$ as $u^{\odot k}$.

We can now prove the following proposition.

Proposition 33.28. *Given a vector space E, if $(e_i)_{i\in I}$ is a basis for E, then the family of vectors*

$$\left(e_{i_1}^{\odot M(i_1)} \odot \cdots \odot e_{i_k}^{\odot M(i_k)}\right)_{\substack{M\in\mathbb{N}^{(I)},\, |M|=m,\\ \{i_1,\ldots,i_k\}=\mathrm{dom}(M)}}$$

is a basis of the symmetric m-th tensor power $\mathrm{S}^m(E)$.

Proof. The proof is very similar to that of Proposition 33.12. First assume that E has finite dimension n. In this case $I = \{1,\ldots,n\}$, and any multiset $M \in \mathbb{N}^{(I)}$ of size $|M| = m$ is of the form $M(m, \{1,\ldots,n\}, k_1,\ldots,k_n)$, with $k_i = M(i)$ and $k_1 + \cdots + k_n = m$.

For any nontrivial vector space F, for any family of vectors

$$(w_M)_{M\in\mathbb{N}^{(I)},\, |M|=m},$$

we show the existence of a symmetric multilinear map $h\colon \mathrm{S}^m(E) \to F$, such that for every $M \in \mathbb{N}^{(I)}$ with $|M| = m$, we have

$$h(e_{i_1}^{\odot M(i_1)} \odot \cdots \odot e_{i_k}^{\odot M(i_k)}) = w_M,$$

where $\{i_1,\ldots,i_k\} = \mathrm{dom}(M)$. We define the map $f\colon E^m \to F$ as follows: for any m vectors $v_1,\ldots,v_m \in E$ we can write $v_k = \sum_{i=1}^n u_{i,k}e_i$ for $k = 1,\ldots,m$ and we set

$$\begin{aligned} &f(v_1,\ldots,v_m)\\ &\quad= \sum_{k_1+\cdots+k_n=m}\left(\sum_{\substack{I_1\cup\cdots\cup I_n=\{1,\ldots,m\}\\ I_i\cap I_j=\emptyset,\, i\neq j,\, |I_j|=k_j}}\left(\prod_{i_1\in I_1} u_{1,i_1}\right)\cdots\left(\prod_{i_n\in I_n} u_{n,i_n}\right)\right)w_{M(m,\{1,\ldots,n\},k_1,\ldots,k_n)}.\end{aligned}$$

It is not difficult to verify that f is symmetric and multilinear. By the universal mapping property of the symmetric tensor product, the linear map $f_\odot\colon \mathrm{S}^m(E) \to F$ such that $f = f_\odot \circ \varphi$, is the desired map h. Then by Proposition 33.4, it follows that the family

$$\left(e_{i_1}^{\odot M(i_1)} \odot \cdots \odot e_{i_k}^{\odot M(i_k)}\right)_{\substack{M\in\mathbb{N}^{(I)},\, |M|=m,\\ \{i_1,\ldots,i_k\}=\mathrm{dom}(M)}}$$

is linearly independent. Using the commutativity of $\odot$, we can also show that these vectors generate $\mathrm{S}^m(E)$, and thus, they form a basis for $\mathrm{S}^m(E)$.

If I is infinite dimensional, then for any m vectors $v_1,\ldots,v_m \in F$ there is a finite subset J of I such that $v_k = \sum_{j\in J} u_{j,k}e_j$ for $k = 1,\ldots,m$, and if we write $n = |J|$, then the formula for $f(v_1,\ldots,v_m)$ is obtained by replacing the set $\{1,\ldots,n\}$ by J. The details are left as an exercise. □

As a consequence, when I is finite, say of size $p = \dim(E)$, the dimension of $\mathrm{S}^m(E)$ is the number of finite multisets $(j_1, \ldots, j_p)$, such that $j_1 + \cdots + j_p = m$, $j_k \geq 0$. We leave as an exercise to show that this number is $\binom{p+m-1}{m}$. Thus, if $\dim(E) = p$, then the dimension of $\mathrm{S}^m(E)$ is $\binom{p+m-1}{m}$. Compare with the dimension of $E^{\otimes m}$, which is p^m. In particular, when $p = 2$, the dimension of $\mathrm{S}^m(E)$ is $m + 1$. This can also be seen directly.

Remark: The number $\binom{p+m-1}{m}$ is also the number of homogeneous monomials

$$X_1^{j_1} \cdots X_p^{j_p}$$

of total degree m in p variables (we have $j_1 + \cdots + j_p = m$). This is not a coincidence! Given a vector space E and a basis $(e_i)_{i \in I}$ for E, Proposition 33.28 shows that every symmetric tensor $z \in \mathrm{S}^m(E)$ can be written in a unique way as

$$z = \sum_{\substack{M \in \mathbb{N}^{(I)} \\ \sum_{i \in I} M(i) = m \\ \{i_1, \ldots, i_k\} = \mathrm{dom}(M)}} \lambda_M \, e_{i_1}^{\odot M(i_1)} \odot \cdots \odot e_{i_k}^{\odot M(i_k)},$$

for some unique family of scalars $\lambda_M \in K$, all zero except for a finite number.

This looks like a homogeneous polynomial of total degree m, where the monomials of total degree m are the symmetric tensors

$$e_{i_1}^{\odot M(i_1)} \odot \cdots \odot e_{i_k}^{\odot M(i_k)}$$

in the "indeterminates" e_i, where $i \in I$ (recall that $M(i_1) + \cdots + M(i_k) = m$) and implies that polynomials can be defined in terms of symmetric tensors.

33.9 Some Useful Isomorphisms for Symmetric Powers

We can show the following property of the symmetric tensor product, using the proof technique of Proposition 33.13 (3).

Proposition 33.29. *We have the following isomorphism:*

$$\mathrm{S}^n(E \oplus F) \cong \bigoplus_{k=0}^{n} \mathrm{S}^k(E) \otimes \mathrm{S}^{n-k}(F).$$

33.10 Duality for Symmetric Powers

In this section all vector spaces are assumed to have *finite dimension over a field of characteristic zero*. We define a nondegenerate pairing $\mathrm{S}^n(E^*) \times \mathrm{S}^n(E) \longrightarrow K$ as follows: Consider the multilinear map

$$(E^*)^n \times E^n \longrightarrow K$$

given by

$$(v_1^*, \ldots, v_n^*, u_1, \ldots, u_n) \mapsto \sum_{\sigma \in \mathfrak{S}_n} v_{\sigma(1)}^*(u_1) \cdots v_{\sigma(n)}^*(u_n).$$

Note that the expression on the right-hand side is "almost" the determinant $\det(v_j^*(u_i))$, except that the sign $\mathrm{sgn}(\sigma)$ is missing (where $\mathrm{sgn}(\sigma)$ is the signature of the permutation σ; that is, the parity of the number of transpositions into which σ can be factored). Such an expression is called a *permanent*.

It can be verified that this expression is symmetric w.r.t. the u_i's and also w.r.t. the v_j^*. For any fixed $(v_1^*, \ldots, v_n^*) \in (E^*)^n$, we get a symmetric multilinear map

$$l_{v_1^*, \ldots, v_n^*} \colon (u_1, \ldots, u_n) \mapsto \sum_{\sigma \in \mathfrak{S}_n} v_{\sigma(1)}^*(u_1) \cdots v_{\sigma(n)}^*(u_n)$$

from E^n to K. The map $l_{v_1^*, \ldots, v_n^*}$ extends uniquely to a linear map $L_{v_1^*, \ldots, v_n^*} \colon \mathrm{S}^n(E) \to K$ making the following diagram commute:

$$\begin{tikzcd}
E^n \arrow[r, "\iota_\odot"] \arrow[dr, "l_{v_1^*, \ldots, v_n^*}"'] & \mathrm{S}^n(E) \arrow[d, "L_{v_1^*, \ldots, v_n^*}"] \\
& K.
\end{tikzcd}$$

We also have the symmetric multilinear map

$$(v_1^*, \ldots, v_n^*) \mapsto L_{v_1^*, \ldots, v_n^*}$$

from $(E^*)^n$ to $\mathrm{Hom}(\mathrm{S}^n(E), K)$, which extends to a linear map L from $\mathrm{S}^n(E^*)$ to $\mathrm{Hom}(\mathrm{S}^n(E), K)$ making the following diagram commute:

$$\begin{tikzcd}
(E^*)^n \arrow[r, "\iota_{\odot^*}"] \arrow[dr] & \mathrm{S}^n(E^*) \arrow[d, "L"] \\
& \mathrm{Hom}(\mathrm{S}^n(E), K).
\end{tikzcd}$$

However, in view of the isomorphism

$$\mathrm{Hom}(U \otimes V, W) \cong \mathrm{Hom}(U, \mathrm{Hom}(V, W)),$$

with $U = \mathrm{S}^n(E^*)$, $V = \mathrm{S}^n(E)$ and $W = K$, we can view L as a linear map

$$L \colon \mathrm{S}^n(E^*) \otimes \mathrm{S}^n(E) \longrightarrow K,$$

which by Proposition 33.8 corresponds to a bilinear map

$$\langle -, - \rangle \colon \mathrm{S}^n(E^*) \times \mathrm{S}^n(E) \longrightarrow K. \tag{$*$}$$

This pairing is given explicitly on generators by

$$\langle v_1^* \odot \cdots \odot v_n^*, u_1, \ldots, u_n \rangle = \sum_{\sigma \in \mathfrak{S}_n} v_{\sigma(1)}^*(u_1) \cdots v_{\sigma(n)}^*(u_n).$$

Now this pairing in nondegenerate. This can be shown using bases.[2] If $(e_1, \ldots, e_m)$ is a basis of E, then for every basis element $(e_{i_1}^*)^{\odot n_1} \odot \cdots \odot (e_{i_k}^*)^{\odot n_k}$ of $\mathrm{S}^n(E^*)$, with $n_1 + \cdots + n_k = n$, we have

$$\langle (e_{i_1}^*)^{\odot n_1} \odot \cdots \odot (e_{i_k}^*)^{\odot n_k}, e_{i_1}^{\odot n_1} \odot \cdots \odot e_{i_k}^{\odot n_k} \rangle = n_1! \cdots n_k!,$$

and

$$\langle (e_{i_1}^*)^{\odot n_1} \odot \cdots \odot (e_{i_k}^*)^{\odot n_k}, e_{j_1} \odot \cdots \odot e_{j_n} \rangle = 0$$

if $(j_1 \ldots, j_n) \neq (\underbrace{i_1, \ldots, i_1}_{n_1}, \ldots, \underbrace{i_k, \ldots, i_k}_{n_k})$.

If the field K has characteristic zero, then $n_1! \cdots n_k! \neq 0$. We leave the details as an exercise to the reader. Therefore we get a canonical isomorphism

$$(\mathrm{S}^n(E))^* \cong \mathrm{S}^n(E^*).$$

The following proposition summarizes the duality properties of symmetric powers.

Proposition 33.30. *Assume the field K has characteristic zero. We have the canonical isomorphisms*

$$(\mathrm{S}^n(E))^* \cong \mathrm{S}^n(E^*)$$

and

$$\mathrm{S}^n(E^*) \cong \mathrm{Sym}^n(E; K) = \mathrm{Hom}_{\mathrm{symlin}}(E^n, K),$$

which allows us to interpret symmetric tensors over E^* as symmetric multilinear maps.

Proof. The isomorphism

$$\mu\colon \mathrm{S}^n(E^*) \cong \mathrm{Sym}^n(E; K)$$

follows from the isomorphisms $(\mathrm{S}^n(E))^* \cong \mathrm{S}^n(E^*)$ and $(\mathrm{S}^n(E))^* \cong \mathrm{Sym}^n(E; K)$ given by Proposition 33.26. □

Remarks:

1. The isomorphism $\mu\colon \mathrm{S}^n(E^*) \cong \mathrm{Sym}^n(E; K)$ discussed above can be described explicitly as the linear extension of the map given by

$$\mu(v_1^* \odot \cdots \odot v_n^*)(u_1, \ldots, u_n) = \sum_{\sigma \in \mathfrak{S}_n} v_{\sigma(1)}^*(u_1) \cdots v_{\sigma(n)}^*(u_n).$$

[2] This is where the assumption that we are in finite dimension and that the field has characteristic zero are used.

If $(e_1, \ldots, e_m)$ is a basis of E, then for every basis element $(e_{i_1}^*)^{\odot n_1} \odot \cdots \odot (e_{i_k}^*)^{\odot n_k}$ of $\mathrm{S}^n(E^*)$, with $n_1 + \cdots + n_k = n$, we have

$$\mu((e_{i_1}^*)^{\odot n_1} \odot \cdots \odot (e_{i_k}^*)^{\odot n_k})(\underbrace{e_{i_1}, \ldots, e_{i_1}}_{n_1} \ldots, \underbrace{e_{i_k}, \ldots, e_{i_k}}_{n_k}) = n_1! \cdots n_k!,$$

If the field K has positive characteristic, then it is possible that $n_1! \cdots n_k! = 0$, and this is why we required K to be of characteristic 0 in order for Proposition 33.30 to hold.

2. The canonical isomorphism of Proposition 33.30 holds under more general conditions. Namely, that K is a commutative algebra with identity over $\mathbb{Q}$, and that the E is a finitely-generated projective K-module (see Definition 35.7). See Bourbaki, [25] (Chapter III, §11, Section 5, Proposition 8).

The map from E^n to $\mathrm{S}^n(E)$ given by $(u_1, \ldots, u_n) \mapsto u_1 \odot \cdots \odot u_n$ yields a surjection $\pi\colon E^{\otimes n} \to \mathrm{S}^n(E)$. Because we are dealing with vector spaces, this map has some section; that is, there is some injection $\eta\colon \mathrm{S}^n(E) \to E^{\otimes n}$ with $\pi \circ \eta = \mathrm{id}$. Since our field K has characteristic 0, there is a special section having a natural definition involving a symmetrization process defined as follows: For every permutation σ, we have the map $r_\sigma\colon E^n \to E^{\otimes n}$ given by

$$r_\sigma(u_1, \ldots, u_n) = u_{\sigma(1)} \otimes \cdots \otimes u_{\sigma(n)}.$$

As r_σ is clearly multilinear, r_σ extends to a linear map $(r_\sigma)_\otimes\colon E^{\otimes n} \to E^{\otimes n}$ making the following diagram commute

$$\begin{tikzcd}
E^n \arrow[r, "\iota_\otimes"] \arrow[dr, "r_\sigma"'] & E^{\otimes n} \arrow[d, "(r_\sigma)_\otimes"] \\
 & E^{\otimes n},
\end{tikzcd}$$

and we get a map $\mathfrak{S}_n \times E^{\otimes n} \longrightarrow E^{\otimes n}$, namely

$$\sigma \cdot z = (r_\sigma)_\otimes(z).$$

It is immediately checked that this is a left action of the symmetric group $\mathfrak{S}_n$ on $E^{\otimes n}$, and the tensors $z \in E^{\otimes n}$ such that

$$\sigma \cdot z = z, \quad \text{for all} \quad \sigma \in \mathfrak{S}_n$$

are called *symmetrized* tensors.

We define the map $\eta\colon E^n \to E^{\otimes n}$ by

$$\eta(u_1, \ldots, u_n) = \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} \sigma \cdot (u_1 \otimes \cdots \otimes u_n) = \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} u_{\sigma(1)} \otimes \cdots \otimes u_{\sigma(n)}.$$

As the right hand side is clearly symmetric, we get a linear map $\eta_\odot \colon \mathrm{S}^n(E) \to E^{\otimes n}$ making the following diagram commute.

$$\begin{tikzcd}
E^n \arrow[r, "\iota_\odot"] \arrow[dr, "\eta"'] & \mathrm{S}^n(E) \arrow[d, "\eta_\odot"] \\
 & E^{\otimes n}
\end{tikzcd}$$

Clearly, $\eta_\odot(\mathrm{S}^n(E))$ is the set of symmetrized tensors in $E^{\otimes n}$. If we consider the map $S = \eta_\odot \circ \pi \colon E^{\otimes n} \longrightarrow E^{\otimes n}$ where π is the surjection $\pi \colon E^{\otimes n} \to \mathrm{S}^n(E)$, it is easy to check that $S \circ S = S$. Therefore, S is a projection, and by linear algebra, we know that

$$E^{\otimes n} = S(E^{\otimes n}) \oplus \operatorname{Ker} S = \eta_\odot(\mathrm{S}^n(E)) \oplus \operatorname{Ker} S.$$

It turns out that $\operatorname{Ker} S = E^{\otimes n} \cap \mathfrak{I} = \operatorname{Ker} \pi$, where $\mathfrak{I}$ is the two-sided ideal of $T(E)$ generated by all tensors of the form $u \otimes v - v \otimes u \in E^{\otimes 2}$ (for example, see Knapp [103], Appendix A). Therefore, $\eta_\odot$ is injective,

$$E^{\otimes n} = \eta_\odot(\mathrm{S}^n(E)) \oplus (E^{\otimes n} \cap \mathfrak{I}) = \eta_\odot(\mathrm{S}^n(E)) \oplus \operatorname{Ker} \pi,$$

and the symmetric tensor power $\mathrm{S}^n(E)$ is naturally embedded into $E^{\otimes n}$.

33.11 Symmetric Algebras

As in the case of tensors, we can pack together all the symmetric powers $\mathrm{S}^n(V)$ into an algebra.

Definition 33.20. Given a vector space V, the space

$$\mathrm{S}(V) = \bigoplus_{m \geq 0} \mathrm{S}^m(V),$$

is called the *symmetric tensor algebra of* V.

We could adapt what we did in Section 33.6 for general tensor powers to symmetric tensors but since we already have the algebra $T(V)$, we can proceed faster. If $\mathfrak{I}$ is the two-sided ideal generated by all tensors of the form $u \otimes v - v \otimes u \in V^{\otimes 2}$, we set

$$\mathrm{S}^\bullet(V) = T(V)/\mathfrak{I}.$$

Observe that since the ideal $\mathfrak{I}$ is generated by elements in $V^{\otimes 2}$, every tensor in $\mathfrak{I}$ is a linear combination of tensors of the form $\omega_1 \otimes (u \otimes v - v \otimes u) \otimes \omega_2$, with $\omega_1 \in V^{\otimes n_1}$ and $\omega_2 \in V^{\otimes n_2}$ for some $n_1, n_2 \in \mathbb{N}$, which implies that

$$\mathfrak{I} = \bigoplus_{m \geq 0} (\mathfrak{I} \cap V^{\otimes m}).$$

Then, $\mathrm{S}^{\bullet}(V)$ automatically inherits a multiplication operation which is commutative, and since $T(V)$ is graded, that is

$$T(V) = \bigoplus_{m\geq 0} V^{\otimes m},$$

we have

$$\mathrm{S}^{\bullet}(V) = \bigoplus_{m\geq 0} V^{\otimes m}/(\mathfrak{I}\cap V^{\otimes m}).$$

However, it is easy to check that

$$\mathrm{S}^{m}(V) \cong V^{\otimes m}/(\mathfrak{I}\cap V^{\otimes m}),$$

so

$$\mathrm{S}^{\bullet}(V) \cong \mathrm{S}(V).$$

When V is of finite dimension n, $\mathrm{S}(V)$ corresponds to *the algebra of polynomials with coefficients in K in n variables* (this can be seen from Proposition 33.28). When V is of infinite dimension and $(u_i)_{i\in I}$ is a basis of V, the algebra $\mathrm{S}(V)$ corresponds to the algebra of polynomials in infinitely many variables in I. What's nice about the symmetric tensor algebra $\mathrm{S}(V)$ is that it provides an intrinsic definition of a polynomial algebra in any set of I variables.

It is also easy to see that $\mathrm{S}(V)$ satisfies the following universal mapping property.

Proposition 33.31. *Given any commutative K-algebra A, for any linear map $f\colon V\to A$, there is a unique K-algebra homomorphism $\overline{f}\colon \mathrm{S}(V)\to A$ so that*

$$f = \overline{f}\circ i,$$

as in the diagram below.

$$\begin{tikzcd}
V \arrow[r, "i"] \arrow[dr, "f"'] & \mathrm{S}(V) \arrow[d, "\overline{f}"] \\
 & A
\end{tikzcd}$$

Remark: If E is finite-dimensional, recall the isomorphism $\mu\colon \mathrm{S}^n(E^*) \longrightarrow \mathrm{Sym}^n(E;K)$ defined as the linear extension of the map given by

$$\mu(v_1^*\odot\cdots\odot v_n^*)(u_1,\ldots,u_n) = \sum_{\sigma\in\mathfrak{S}_n} v_{\sigma(1)}^*(u_1)\cdots v_{\sigma(n)}^*(u_n).$$

Now we have also a multiplication operation $\mathrm{S}^m(E^*)\times\mathrm{S}^n(E^*)\longrightarrow\mathrm{S}^{m+n}(E^*)$. The following question then arises:

Can we define a multiplication $\mathrm{Sym}^m(E;K) \times \mathrm{Sym}^n(E;K) \longrightarrow \mathrm{Sym}^{m+n}(E;K)$ directly on symmetric multilinear forms, so that the following diagram commutes?

$$\begin{tikzcd}
\mathrm{S}^m(E^*) \times \mathrm{S}^n(E^*) \arrow[r, "\odot"] \arrow[d, "\mu_m \times \mu_n"] & \mathrm{S}^{m+n}(E^*) \arrow[d, "\mu_{m+n}"] \\
\mathrm{Sym}^m(E;K) \times \mathrm{Sym}^n(E;K) \arrow[r, "\cdot"] & \mathrm{Sym}^{m+n}(E;K)
\end{tikzcd}$$

The answer is *yes*! The solution is to define this multiplication such that for $f \in \mathrm{Sym}^m(E;K)$ and $g \in \mathrm{Sym}^n(E;K)$,

$$(f \cdot g)(u_1, \ldots, u_{m+n}) = \sum_{\sigma \in \mathrm{shuffle}(m,n)} f(u_{\sigma(1)}, \ldots, u_{\sigma(m)}) g(u_{\sigma(m+1)}, \ldots, u_{\sigma(m+n)}), \qquad (*)$$

where shuffle(m,n) consists of all (m,n)-"shuffles;" that is, permutations σ of $\{1, \ldots m+n\}$ such that $\sigma(1) < \cdots < \sigma(m)$ and $\sigma(m+1) < \cdots < \sigma(m+n)$. Observe that a (m,n)-shuffle is completely determined by the sequence $\sigma(1) < \cdots < \sigma(m)$.

For example, suppose $m = 2$ and $n = 1$. Given $v_1^*, v_2^*, v_3^* \in E^*$, the multiplication structure on $\mathrm{S}(E^*)$ implies that $(v_1^* \odot v_2^*) \cdot v_3^* = v_1^* \odot v_2^* \odot v_3^* \in \mathrm{S}^3(E^*)$. Furthermore, for $u_1, u_2, u_3, \in E$,

$$\begin{aligned}
\mu_3(v_1^* \odot v_2^* \odot v_3^*)(u_1, u_2, u_3) &= \sum_{\sigma \in \mathfrak{S}_3} v^*_{\sigma(1)}(u_1) v^*_{\sigma(2)}(u_2) v^*_{\sigma(3)}(u_3) \\
&= v_1^*(u_1) v_2^*(u_2) v_3^*(u_3) + v_1^*(u_1) v_3^*(u_2) v_2^*(u_3) \\
&\quad + v_2^*(u_1) v_1^*(u_2) v_3^*(u_3) + v_2^*(u_1) v_3^*(u_2) v_1^*(u_3) \\
&\quad + v_3^*(u_1) v_1^*(u_2) v_2^*(u_3) + v_3^*(u_1) v_2^*(u_2) v_1^*(u_3).
\end{aligned}$$

Now the $(2,1)$- shuffles of $\{1,2,3\}$ are the following three permutations, namely

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

If $f \cong \mu_2(v_1^* \odot v_2^*)$ and $g \cong \mu_1(v_3^*)$, then $(*)$ implies that

$$\begin{aligned}
(f \cdot g)(u_1, u_2, u_3) &= \sum_{\sigma \in \mathrm{shuffle}(2,1)} f(u_{\sigma(1)}, u_{\sigma(2)}) g(u_{\sigma(3)}) \\
&= f(u_1, u_2) g(u_3) + f(u_1, u_3) g(u_2) + f(u_2, u_3) g(u_1) \\
&= \mu_2(v_1^* \odot v_2^*)(u_1, u_2) \mu_1(v_3^*)(u_3) + \mu_2(v_1^* \odot v_2^*)(u_1, u_3) \mu_1(v_3^*)(u_2) \\
&\quad + \mu_2(v_1^* \odot v_2^*)(u_2, u_3) \mu_1(v_3^*)(u_1) \\
&= (v_1^*(u_1) v_2^*(u_2) + v_2^*(u_1) v_1^*(u_2)) v_3^*(u_3) \\
&\quad + (v_1^*(u_1) v_2^*(u_3) + v_2^*(u_1) v_1^*(u_3)) v_3^*(u_2) \\
&\quad + (v_1^*(u_2) v_2^*(u_3) + v_2^*(u_2) v_1^*(u_3)) v_3^*(u_1) \\
&= \mu_3(v_1^* \odot v_2^* \odot v_3^*)(u_1, u_2, u_3).
\end{aligned}$$

We leave it as an exercise for the reader to verify Equation $(*)$ for arbitrary nonnegative integers m and n.

Another useful canonical isomorphism (of K-algebras) is given below.

Proposition 33.32. *For any two vector spaces E and F, there is a canonical isomorphism (of K-algebras)*

$$\mathrm{S}(E \oplus F) \cong \mathrm{S}(E) \otimes \mathrm{S}(F).$$

33.12 Problems

Problem 33.1. Prove Proposition 33.4.

Problem 33.2. Given two linear maps $f\colon E \to E'$ and $g\colon F \to F'$, we defined the unique linear map

$$f \otimes g\colon E \otimes F \to E' \otimes F'$$

by

$$(f \otimes g)(u \otimes v) = f(u) \otimes g(v),$$

for all $u \in E$ and all $v \in F$. See Proposition 33.9. Thus $f \otimes g \in \mathrm{Hom}(E \otimes F, E' \otimes F')$. If we denote the tensor product $E \otimes F$ by $T(E, F)$, and we assume that E, E' and F, F' are finite dimensional, pick bases and show that the map induced by $f \otimes g \mapsto T(f, g)$ is an isomorphism

$$\mathrm{Hom}(E, F) \otimes \mathrm{Hom}(E', F') \cong \mathrm{Hom}(E \otimes F, E' \otimes F').$$

Problem 33.3. Adjust the proof of Proposition 33.13 (2) to show that

$$E \otimes (F \otimes G) \cong E \otimes F \otimes G,$$

whenever E, F, and G are arbitrary vector spaces.

Problem 33.4. Given a fixed vector space G, for any two vector spaces M and N and every linear map $f\colon M \to N$, we defined $\tau_G(f) = f \otimes \mathrm{id}_G$ to be the unique linear map making the following diagram commute.

$$\begin{tikzcd}
M \times G \arrow[r, "\iota_{M\otimes}"] \arrow[d, "f\times \mathrm{id}_G"'] & M \otimes G \arrow[d, "f\otimes \mathrm{id}_G"] \\
N \times G \arrow[r, "\iota_{N\otimes}"'] & N \otimes G
\end{tikzcd}$$

See the proof of Proposition 33.13 (3). Show that

(1) $\tau_G(0) = 0$,

(2) $\tau_G(\mathrm{id}_M) = (\mathrm{id}_M \otimes \mathrm{id}_G) = \mathrm{id}_{M\otimes G}$,

(3) If $f'\colon M \to N$ is another linear map, then $\tau_G(f + f') = \tau_G(f) + \tau_G(f')$.

Problem 33.5. Induct on $m \geq 2$ to prove the canonical isomorphism

$$V^{\otimes m} \otimes V^{\otimes n} \cong V^{\otimes (m+n)}.$$

Use this isomorphism to show that $\cdot\colon V^{\otimes m} \times V^{\otimes n} \longrightarrow V^{\otimes (m+n)}$ defined as

$$(v_1 \otimes \cdots \otimes v_m) \cdot (w_1 \otimes \cdots \otimes w_n) = v_1 \otimes \cdots \otimes v_m \otimes w_1 \otimes \cdots \otimes w_n.$$

induces a multiplication on $T(V)$.
Hint. See Jacobson [96], Section 3.9, or Bertin [15], Chapter 4, Section 2.).

Problem 33.6. Prove Proposition 33.19.
Hint. See Knapp [103] (Appendix A, Proposition A.14) or Bertin [15] (Chapter 4, Theorem 2.4).

Problem 33.7. Given linear maps $f'\colon E' \to E''$ and $g'\colon E' \to E''$, show that

$$(f' \circ f) \odot (g' \circ g) = (f' \odot g') \circ (f \odot g).$$

Problem 33.8. Complete the proof of Proposition 33.28 for the case of an infinite dimensional vector space E.

Problem 33.9. Let I be a finite index set of cardinality p. Let m be a nonnegative integer. Show that the number of multisets over I with cardinality m is $\binom{p+m-1}{m}$.

Problem 33.10. Prove Proposition 33.29.

Problem 33.11. Using bases, show that the bilinear map at $(*)$ in Section 33.10 produces a nondegenerate pairing.

Problem 33.12. Let $\mathfrak{I}$ be the two-sided ideal generated by all tensors of the form $u \otimes v - v \otimes u \in V^{\otimes 2}$. Prove that $\mathrm{S}^m(V) \cong V^{\otimes m}/(\mathfrak{I} \cap V^{\otimes m})$.

Problem 33.13. Verify Equation $(*)$ of Section 33.11 for arbitrary nonnegative integers m and n.

Chapter 34

Exterior Tensor Powers and Exterior Algebras

34.1 Exterior Tensor Powers

In this chapter we consider *alternating* (also called *skew-symmetric*) multilinear maps and *exterior tensor powers* (also called *alternating tensor powers*), denoted $\bigwedge^n(E)$. In many respects alternating multilinear maps and exterior tensor powers can be treated much like symmetric tensor powers, except that $\mathrm{sgn}(\sigma)$ needs to be inserted in front of the formulae valid for symmetric powers.

Roughly speaking, we are now in the world of determinants rather than in the world of permanents. However, there are also some fundamental differences, one of which being that the exterior tensor power $\bigwedge^n(E)$ is the trivial vector space (0) when E is finite-dimensional and when $n > \dim(E)$. This chapter provides the firm foundations for understanding differential forms.

As in the case of symmetric tensor powers, since we already have the tensor algebra $T(V)$, we can proceed rather quickly. But first let us review some basic definitions and facts.

Definition 34.1. Let $f\colon E^n \to F$ be a multilinear map. We say that f *alternating* iff for all $u_i \in E$, $f(u_1, \ldots, u_n) = 0$ whenever $u_i = u_{i+1}$, for some i with $1 \leq i \leq n-1$; that is, $f(u_1, \ldots, u_n) = 0$ whenever two adjacent arguments are identical. We say that f is *skew-symmetric* (or *anti-symmetric*) iff

$$f(u_{\sigma(1)}, \ldots, u_{\sigma(n)}) = \mathrm{sgn}(\sigma) f(u_1, \ldots, u_n),$$

for every permutation $\sigma \in \mathfrak{S}_n$, and all $u_i \in E$.

For $n = 1$, we agree that every linear map $f\colon E \to F$ is alternating. The vector space of all multilinear alternating maps $f\colon E^n \to F$ is denoted $\mathrm{Alt}^n(E; F)$. Note that $\mathrm{Alt}^1(E; F) = \mathrm{Hom}(E, F)$. The following basic proposition shows the relationship between alternation and skew-symmetry.

Proposition 34.1. *Let $f\colon E^n \to F$ be a multilinear map. If f is alternating, then the following properties hold:*

(1) For all i, with $1 \leq i \leq n-1$,

$$f(\ldots, u_i, u_{i+1}, \ldots) = -f(\ldots, u_{i+1}, u_i, \ldots).$$

(2) For every permutation $\sigma \in \mathfrak{S}_n$,

$$f(u_{\sigma(1)}, \ldots, u_{\sigma(n)}) = \mathrm{sgn}(\sigma) f(u_1, \ldots, u_n).$$

(3) For all i, j, with $1 \leq i < j \leq n$,

$$f(\ldots, u_i, \ldots u_j, \ldots) = 0 \quad \textit{whenever } u_i = u_j.$$

Moreover, if our field K has characteristic different from 2, then every skew-symmetric multilinear map is alternating.

Proof. (1) By multilinearity applied twice, we have

$$\begin{aligned} f(\ldots, u_i + u_{i+1}, u_i + u_{i+1}, \ldots) = f(\ldots, u_i, u_i, \ldots) + f(\ldots, u_i, u_{i+1}, \ldots) \\ + f(\ldots, u_{i+1}, u_i, \ldots) + f(\ldots, u_{i+1}, u_{i+1}, \ldots). \end{aligned}$$

Since f is alternating, we get

$$0 = f(\ldots, u_i, u_{i+1}, \ldots) + f(\ldots, u_{i+1}, u_i, \ldots);$$

that is, $f(\ldots, u_i, u_{i+1}, \ldots) = -f(\ldots, u_{i+1}, u_i, \ldots)$.

(2) Clearly, the symmetric group, $\mathfrak{S}_n$, acts on $\mathrm{Alt}^n(E; F)$ on the left, *via*

$$\sigma \cdot f(u_1, \ldots, u_n) \; = f(u_{\sigma(1)}, \ldots, u_{\sigma(n)}).$$

Consequently, as $\mathfrak{S}_n$ is generated by the transpositions (permutations that swap exactly two elements), since for a transposition, (2) is simply (1), we deduce (2) by induction on the number of transpositions in σ.

(3) There is a permutation σ that sends u_i and u_j respectively to u_1 and u_2. By hypothesis $u_i = u_j$, so we have $u_{\sigma(1)} = u_{\sigma(2)}$, and as f is alternating we have

$$f(u_{\sigma(1)}, \ldots, u_{\sigma(n)}) = 0.$$

However, by (2),

$$f(u_1, \ldots, u_n) = \mathrm{sgn}(\sigma) f(u_{\sigma(1)}, \ldots, u_{\sigma(n)}) = 0.$$

Now when f is skew-symmetric, if σ is the transposition swapping u_i and $u_{i+1} = u_i$, as $\mathrm{sgn}(\sigma) = -1$, we get

$$f(\ldots, u_i, u_i, \ldots) = -f(\ldots, u_i, u_i, \ldots),$$

so that

$$2f(\dots, u_i, u_i, \dots) = 0,$$

and in every characteristic except 2, we conclude that $f(\dots, u_i, u_i, \dots) = 0$, namely f is alternating. □

Proposition 34.1 shows that in every characteristic except 2, alternating and skew-symmetric multilinear maps are identical. Using Proposition 34.1 we easily deduce the following crucial fact.

Proposition 34.2. *Let $f\colon E^n \to F$ be an alternating multilinear map. For any families of vectors, $(u_1, \dots, u_n)$ and $(v_1, \dots, v_n)$, with $u_i, v_i \in E$, if*

$$v_j = \sum_{i=1}^{n} a_{ij} u_i, \qquad 1 \leq j \leq n,$$

then

$$f(v_1, \dots, v_n) = \left(\sum_{\sigma \in \mathfrak{S}_n} \mathrm{sgn}(\sigma)\, a_{\sigma(1),1} \cdots a_{\sigma(n),n}\right) f(u_1, \dots, u_n) = \det(A) f(u_1, \dots, u_n),$$

where A is the $n \times n$ matrix, $A = (a_{ij})$.

Proof. Use Property (ii) of Proposition 34.1. □

We are now ready to define and construct exterior tensor powers.

Definition 34.2. An *n-th exterior tensor power* of a vector space E, where $n \geq 1$, is a vector space A together with an alternating multilinear map $\varphi\colon E^n \to A$, such that for every vector space F and for every alternating multilinear map $f\colon E^n \to F$, there is a unique linear map $f_\wedge\colon A \to F$ with

$$f(u_1, \dots, u_n) = f_\wedge(\varphi(u_1, \dots, u_n)),$$

for all $u_1, \dots, u_n \in E$, or for short

$$f = f_\wedge \circ \varphi.$$

Equivalently, there is a unique linear map $f_\wedge$ such that the following diagram commutes:

$$\begin{tikzcd}
E^n \arrow[r, "\varphi"] \arrow[dr, "f"'] & A \arrow[d, "f_\wedge"] \\
& F.
\end{tikzcd}$$

The above property is called the *universal mapping property* of the exterior tensor power (A, φ).

We now show that any two n-th exterior tensor powers (A_1, φ_1) and (A_2, φ_2) for E are isomorphic.

Proposition 34.3. *Given any two n-th exterior tensor powers (A_1, φ_1) and (A_2, φ_2) for E, there is an isomorphism $h\colon A_1 \to A_2$ such that*

$$\varphi_2 = h \circ \varphi_1.$$

Proof. Replace tensor product by n-th exterior tensor power in the proof of Proposition 33.5. □

We next give a construction that produces an n-th exterior tensor power of a vector space E.

Theorem 34.4. *Given a vector space E, an n-th exterior tensor power $(\bigwedge^n(E), \varphi)$ for E can be constructed ($n \geq 1$). Furthermore, denoting $\varphi(u_1, \ldots, u_n)$ as $u_1 \wedge \cdots \wedge u_n$, the exterior tensor power $\bigwedge^n(E)$ is generated by the vectors $u_1 \wedge \cdots \wedge u_n$, where $u_1, \ldots, u_n \in E$, and for every alternating multilinear map $f\colon E^n \to F$, the unique linear map $f_\wedge\colon \bigwedge^n(E) \to F$ such that $f = f_\wedge \circ \varphi$ is defined by*

$$f_\wedge(u_1 \wedge \cdots \wedge u_n) = f(u_1, \ldots, u_n)$$

on the generators $u_1 \wedge \cdots \wedge u_n$ of $\bigwedge^n(E)$.

Proof sketch. We can give a quick proof using the tensor algebra $T(E)$. Let $\mathfrak{I}_a$ be the two-sided ideal of $T(E)$ generated by all tensors of the form $u \otimes u \in E^{\otimes 2}$. Then let

$$\bigwedge^n(E) = E^{\otimes n}/(\mathfrak{I}_a \cap E^{\otimes n})$$

and let π be the projection $\pi\colon E^{\otimes n} \to \bigwedge^n(E)$. If we let $u_1 \wedge \cdots \wedge u_n = \pi(u_1 \otimes \cdots \otimes u_n)$, it is easy to check that $(\bigwedge^n(E), \wedge)$ satisfies the conditions of Theorem 34.4. □

Remark: We can also define

$$\bigwedge(E) = T(E)/\mathfrak{I}_a = \bigoplus_{n \geq 0} \bigwedge^n(E),$$

the *exterior algebra* of E. This is the skew-symmetric counterpart of $\mathrm{S}(E)$, and we will study it a little later.

For simplicity of notation, we may write $\bigwedge^n E$ for $\bigwedge^n(E)$. We also abbreviate "exterior tensor power" as "exterior power." Clearly, $\bigwedge^1(E) \cong E$, and it is convenient to set $\bigwedge^0(E) = K$.

The fact that the map $\varphi\colon E^n \to \bigwedge^n(E)$ is alternating and multilinear can also be expressed as follows:

$$\begin{aligned}
u_1 \wedge \cdots \wedge (u_i + v_i) \wedge \cdots \wedge u_n &= (u_1 \wedge \cdots \wedge u_i \wedge \cdots \wedge u_n) \\
&\quad + (u_1 \wedge \cdots \wedge v_i \wedge \cdots \wedge u_n), \\
u_1 \wedge \cdots \wedge (\lambda u_i) \wedge \cdots \wedge u_n &= \lambda(u_1 \wedge \cdots \wedge u_i \wedge \cdots \wedge u_n), \\
u_{\sigma(1)} \wedge \cdots \wedge u_{\sigma(n)} &= \mathrm{sgn}(\sigma)\, u_1 \wedge \cdots \wedge u_n,
\end{aligned}$$

for all $\sigma \in \mathfrak{S}_n$.

The map φ from E^n to $\bigwedge^n(E)$ is often denoted $\iota_\wedge$, so that

$$\iota_\wedge(u_1, \ldots, u_n) = u_1 \wedge \cdots \wedge u_n.$$

Theorem 34.4 implies the following result.

Proposition 34.5. *There is a canonical isomorphism*

$$\mathrm{Hom}(\bigwedge^n(E), F) \cong \mathrm{Alt}^n(E; F)$$

between the vector space of linear maps $\mathrm{Hom}(\bigwedge^n(E), F)$ *and the vector space of alternating multilinear maps* $\mathrm{Alt}^n(E; F)$*, given by the linear map* $- \circ \varphi$ *defined by* $\mapsto h \circ \varphi$*, with* $h \in \mathrm{Hom}(\bigwedge^n(E), F)$*. In particular, when* $F = K$*, we get a canonical isomorphism*

$$\left(\bigwedge^n(E)\right)^* \cong \mathrm{Alt}^n(E; K).$$

Definition 34.3. Tensors $\alpha \in \bigwedge^n(E)$ are called *alternating n-tensors* or *alternating tensors of degree n* and we write $\deg(\alpha) = n$. Tensors of the form $u_1 \wedge \cdots \wedge u_n$, where $u_i \in E$, are called *simple (or decomposable) alternating n-tensors*. Those alternating n-tensors that are not simple are often called *compound alternating n-tensors*. Simple tensors $u_1 \wedge \cdots \wedge u_n \in \bigwedge^n(E)$ are also called *n-vectors* and tensors in $\bigwedge^n(E^*)$ are often called *(alternating) n-forms*.

Given two linear maps $f\colon E \to E'$ and $g\colon E \to E'$, since the map $\iota'_\wedge \circ (f \times g)$ is bilinear and alternating, there is a unique linear map $f \wedge g\colon \bigwedge^2(E) \to \bigwedge^2(E')$ making the following diagram commute:

$$\begin{tikzcd}
E^2 \arrow[r, "\iota_\wedge"] \arrow[d, "f\times g"'] & \bigwedge^2(E) \arrow[d, "f\wedge g"] \\
(E')^2 \arrow[r, "\iota'_\wedge"'] & \bigwedge^2(E').
\end{tikzcd}$$

The map $f \wedge g\colon \bigwedge^2(E) \to \bigwedge^2(E')$ is determined by

$$(f \wedge g)(u \wedge v) = f(u) \wedge g(u).$$

Proposition 34.6. *Given any linear maps $f\colon E \to E'$, $g\colon E \to E'$, $f'\colon E' \to E''$ and $g'\colon E' \to E''$, we have*

$$(f' \circ f) \wedge (g' \circ g) = (f' \wedge g') \circ (f \wedge g).$$

The generalization to the alternating product $f_1 \wedge \cdots \wedge f_n$ of $n \geq 3$ linear maps $f_i\colon E \to E'$ is immediate, and left to the reader.

34.2 Bases of Exterior Powers

Definition 34.4. Let E be any vector space. For any basis $(u_i)_{i\in\Sigma}$ for E, we assume that some total ordering $\leq$ on the index set Σ has been chosen. Call the pair $((u_i)_{i\in\Sigma}, \leq)$ an *ordered basis*. Then for any nonempty finite subset $I \subseteq \Sigma$, let

$$u_I = u_{i_1} \wedge \cdots \wedge u_{i_m},$$

where $I = \{i_1, \ldots, i_m\}$, with $i_1 < \cdots < i_m$.

Since $\bigwedge^n(E)$ is generated by the tensors of the form $v_1 \wedge \cdots \wedge v_n$, with $v_i \in E$, in view of skew-symmetry, it is clear that the tensors u_I with $|I| = n$ generate $\bigwedge^n(E)$ (where $((u_i)_{i\in\Sigma}, \leq)$ is an ordered basis). Actually they form a basis. To gain an intuitive understanding of this statement, let $m = 2$ and E be a 3-dimensional vector space lexicographically ordered basis $\{e_1, e_2, e_3\}$. We claim that

$$e_1 \wedge e_2, \qquad e_1 \wedge e_3, \qquad e_2 \wedge e_3$$

form a basis for $\bigwedge^2(E)$ since they not only generate $\bigwedge^2(E)$ but are linearly independent. The linear independence is argued as follows: given any vector space F, if w_{12}, w_{13}, w_{23} are any vectors in F, there is an alternating bilinear map $h\colon E^2 \to F$ such that

$$h(e_1, e_2) = w_{12}, \qquad h(e_1, e_3) = w_{13}, \qquad h(e_2, e_3) = w_{23}.$$

Because h yields a unique linear map $h_\wedge\colon \bigwedge^2 E \to F$ such that

$$h_\wedge(e_i \wedge e_j) = w_{ij}, \quad 1 \leq i < j \leq 3,$$

by Proposition 33.4, the vectors

$$e_1 \wedge e_2, \qquad e_1 \wedge e_3, \qquad e_2 \wedge e_3$$

are linearly independent. This suggests understanding how an alternating bilinear function $f\colon E^2 \to F$ is expressed in terms of its values $f(e_i, e_j)$ on the basis vectors (e_1, e_2, e_3). Using bilinearity and alternation, we obtain

$$\begin{aligned} f(u_1e_1 + u_2e_2 + u_3e_3, v_1e_1 + v_2e_2 + v_3e_3) &= (u_1v_2 - u_2v_1)f(e_1, e_2) + (u_1v_3 - u_3v_1)f(e_1, e_3) \\ &\quad + (u_2v_3 - u_3v_2)f(e_2, e_3). \end{aligned}$$

Therefore, given $w_{12}, w_{13}, w_{23} \in F$, the function h given by

$$\begin{aligned} h(u_1e_1 + u_2e_2 + u_3e_3, v_1e_1 + v_2e_2 + v_3e_3) &= (u_1v_2 - u_2v_1)w_{12} + (u_1v_3 - u_3v_1)w_{13} \\ &\quad + (u_2v_3 - u_3v_2)w_{23} \end{aligned}$$

is clearly bilinear and alternating, and by construction $h(e_i, e_j) = w_{ij}$, with $1 \leq i < j \leq 3$ does the job.

We now prove the assertion that tensors u_I with $|I| = n$ generate $\bigwedge^n(E)$ for arbitrary n.

Proposition 34.7. *Given any vector space E, if E has finite dimension $d = \dim(E)$, then for all $n > d$, the exterior power $\bigwedge^n(E)$ is trivial; that is $\bigwedge^n(E) = (0)$. If $n \leq d$ or if E is infinite dimensional, then for every ordered basis $((u_i)_{i\in\Sigma}, \leq)$, the family (u_I) is basis of $\bigwedge^n(E)$, where I ranges over finite nonempty subsets of Σ of size $|I| = n$.*

Proof. First assume that E has finite dimension $d = \dim(E)$ and that $n > d$. We know that $\bigwedge^n(E)$ is generated by the tensors of the form $v_1 \wedge \cdots \wedge v_n$, with $v_i \in E$. If $u_1, \ldots, u_d$ is a basis of E, as every v_i is a linear combination of the u_j, when we expand $v_1 \wedge \cdots \wedge v_n$ using multilinearity, we get a linear combination of the form

$$v_1 \wedge \cdots \wedge v_n = \sum_{(j_1,\ldots,j_n)} \lambda_{(j_1,\ldots,j_n)}\, u_{j_1} \wedge \cdots \wedge u_{j_n},$$

where each $(j_1, \ldots, j_n)$ is some sequence of integers $j_k \in \{1, \ldots, d\}$. As $n > d$, each sequence $(j_1, \ldots, j_n)$ must contain two identical elements. By alternation, $u_{j_1} \wedge \cdots \wedge u_{j_n} = 0$, and so $v_1 \wedge \cdots \wedge v_n = 0$. It follows that $\bigwedge^n(E) = (0)$.

Now assume that either $\dim(E) = d$ and $n \leq d$, or that E is infinite dimensional. The argument below shows that the u_I are nonzero and linearly independent. As usual, let $u_i^* \in E^*$ be the linear form given by

$$u_i^*(u_j) = \delta_{ij}.$$

For any nonempty subset $I = \{i_1, \ldots, i_n\} \subseteq \Sigma$ with $i_1 < \cdots < i_n$, for any n vectors $v_1, \ldots, v_n \in E$, let

$$l_I(v_1, \ldots, v_n) = \det(u_{i_j}^*(v_k)) = \begin{vmatrix} u_{i_1}^*(v_1) & \cdots & u_{i_1}^*(v_n) \\ \vdots & \ddots & \vdots \\ u_{i_n}^*(v_1) & \cdots & u_{i_n}^*(v_n) \end{vmatrix}.$$

If we let the n-tuple $(v_1, \ldots, v_n)$ vary we obtain a map l_I from E^n to K, and it is easy to check that this map is alternating multilinear. Thus l_I induces a unique linear map $L_I \colon \bigwedge^n(E) \to K$ making the following diagram commute.

$$\begin{tikzcd} E^n \arrow[r, "\iota_\wedge"] \arrow[rd, "l_I"'] & \bigwedge^n(E) \arrow[d, "L_I"] \\ & K \end{tikzcd}$$

Observe that for any nonempty finite subset $J \subseteq \Sigma$ with $|J| = n$, we have

$$L_I(u_J) = \begin{cases} 1 & \text{if } I = J \\ 0 & \text{if } I \neq J. \end{cases}$$

Note that when $\dim(E) = d$ and $n \leq d$, or when E is infinite-dimensional, the forms $u^*_{i_1}, \ldots, u^*_{i_n}$ are all distinct, so the above does hold. Since $L_I(u_I) = 1$, we conclude that $u_I \neq 0$. If we have a linear combination

$$\sum_I \lambda_I u_I = 0,$$

where the above sum is finite and involves nonempty finite subset $I \subseteq \Sigma$ with $|I| = n$, for every such I, when we apply L_I we get $\lambda_I = 0$, proving linear independence. □

As a corollary, if E is finite dimensional, say $\dim(E) = d$, and if $1 \leq n \leq d$, then we have

$$\dim(\bigwedge^n(E)) = \binom{n}{d},$$

and if $n > d$, then $\dim(\bigwedge^n(E)) = 0$.

Remark: When $n = 0$, if we set $u_\emptyset = 1$, then $(u_\emptyset) = (1)$ is a basis of $\bigwedge^0(V) = K$.

It follows from Proposition 34.7 that the family $(u_I)_I$ where $I \subseteq \Sigma$ ranges over finite subsets of Σ is a basis of $\bigwedge(V) = \bigoplus_{n\geq 0} \bigwedge^n(V)$.

As a corollary of Proposition 34.7 we obtain the following useful criterion for linear independence.

Proposition 34.8. *For any vector space E, the vectors $u_1, \ldots, u_n \in E$ are linearly independent iff $u_1 \wedge \cdots \wedge u_n \neq 0$.*

Proof. If $u_1 \wedge \cdots \wedge u_n \neq 0$, then $u_1, \ldots, u_n$ must be linearly independent. Otherwise, some u_i would be a linear combination of the other u_j's (with $j \neq i$), and then, as in the proof of Proposition 34.7, $u_1 \wedge \cdots \wedge u_n$ would be a linear combination of wedges in which two vectors are identical, and thus zero.

Conversely, assume that $u_1, \ldots, u_n$ are linearly independent. Then we have the linear forms $u^*_i \in E^*$ such that

$$u^*_i(u_j) = \delta_{i,j} \qquad 1 \leq i, j \leq n.$$

As in the proof of Proposition 34.7, we have a linear map $L_{u_1,\ldots,u_n} \colon \bigwedge^n(E) \to K$ given by

$$L_{u_1,\ldots,u_n}(v_1 \wedge \cdots \wedge v_n) = \det(u^*_j(v_i)) = \begin{vmatrix} u^*_1(v_1) & \cdots & u^*_1(v_n) \\ \vdots & \ddots & \vdots \\ u^*_n(v_1) & \cdots & u^*_n(v_n) \end{vmatrix},$$

for all $v_1 \wedge \cdots \wedge v_n \in \bigwedge^n(E)$. As $L_{u_1,\ldots,u_n}(u_1 \wedge \cdots \wedge u_n) = 1$, we conclude that $u_1 \wedge \cdots \wedge u_n \neq 0$. □

Proposition 34.8 shows that *geometrically every nonzero wedge $u_1 \wedge \cdots \wedge u_n$ corresponds to some oriented version of an n-dimensional subspace of E.*

34.3 Some Useful Isomorphisms for Exterior Powers

We can show the following property of the exterior tensor product, using the proof technique of Proposition 33.13.

Proposition 34.9. *We have the following isomorphism:*

$$\bigwedge^n(E \oplus F) \cong \bigoplus_{k=0}^{n} \bigwedge^k(E) \otimes \bigwedge^{n-k}(F).$$

34.4 Duality for Exterior Powers

In this section *all vector spaces are assumed to have finite dimension.* We define a nondegenerate pairing $\bigwedge^n(E^*) \times \bigwedge^n(E) \longrightarrow K$ as follows: Consider the multilinear map

$$(E^*)^n \times E^n \longrightarrow K$$

given by

$$\begin{aligned}(v_1^*, \ldots, v_n^*, u_1, \ldots, u_n) \mapsto \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma)\, v_{\sigma(1)}^*(u_1) \cdots v_{\sigma(n)}^*(u_n) &= \det(v_j^*(u_i)) \\ &= \begin{vmatrix} v_1^*(u_1) & \cdots & v_1^*(u_n) \\ \vdots & \ddots & \vdots \\ v_n^*(u_1) & \cdots & v_n^*(u_n) \end{vmatrix}.\end{aligned}$$

It is easily checked that this expression is alternating w.r.t. the u_i's and also w.r.t. the v_j^*. For any fixed $(v_1^*, \ldots, v_n^*) \in (E^*)^n$, we get an alternating multilinear map

$$l_{v_1^*, \ldots, v_n^*} \colon (u_1, \ldots, u_n) \mapsto \det(v_j^*(u_i))$$

from E^n to K. The map $l_{v_1^*, \ldots, v_n^*}$ extends uniquely to a linear map $L_{v_1^*, \ldots, v_n^*} \colon \bigwedge^n(E) \to K$ making the following diagram commute:

$$\begin{tikzcd} E^n \arrow[r, "\iota_\wedge"] \arrow[dr, "l_{v_1^*, \ldots, v_n^*}"'] & \bigwedge^n(E) \arrow[d, "L_{v_1^*, \ldots, v_n^*}"] \\ & K. \end{tikzcd}$$

We also have the alternating multilinear map

$$(v_1^*, \ldots, v_n^*) \mapsto L_{v_1^*, \ldots, v_n^*}$$

from $(E^*)^n$ to $\mathrm{Hom}(\bigwedge^n(E), K)$, which extends to a linear map L from $\bigwedge^n(E^*)$ to $\mathrm{Hom}(\bigwedge^n(E), K)$ making the following diagram commute:

$$\begin{tikzcd}
(E^*)^n \arrow[r, "\iota_{\wedge^*}"] \arrow[dr] & \bigwedge^n(E^*) \arrow[d, "L"] \\
 & \mathrm{Hom}(\bigwedge^n(E), K).
\end{tikzcd}$$

However, in view of the isomorphism

$$\mathrm{Hom}(U \otimes V, W) \cong \mathrm{Hom}(U, \mathrm{Hom}(V, W)),$$

with $U = \bigwedge^n(E^*)$, $V = \bigwedge^n(E)$ and $W = K$, we can view L as a linear map

$$L\colon \bigwedge^n(E^*) \otimes \bigwedge^n(E) \longrightarrow K,$$

which by Proposition 33.8 corresponds to a bilinear map

$$\langle -, - \rangle\colon \bigwedge^n(E^*) \times \bigwedge^n(E) \longrightarrow K. \qquad (*)$$

This pairing is given explicitly in terms of generators by

$$\langle v_1^* \wedge \cdots \wedge v_n^*, u_1, \ldots, u_n \rangle = \det(v_j^*(u_i)).$$

Now this pairing in nondegenerate. This can be shown using bases. Given any basis $(e_1, \ldots, e_m)$ of E, for every basis element $e_{i_1}^* \wedge \cdots \wedge e_{i_n}^*$ of $\bigwedge^n(E^*)$ (with $1 \leq i_1 < \cdots < i_n \leq m$), we have

$$\langle e_{i_1}^* \wedge \cdots \wedge e_{i_n}^*, e_{j_1}, \ldots, e_{j_n} \rangle = \begin{cases} 1 & \text{if } (j_1, \ldots, j_n) = (i_1, \ldots, i_n) \\ 0 & \text{otherwise.} \end{cases}$$

We leave the details as an exercise to the reader. As a consequence we get the following canonical isomorphisms.

Proposition 34.10. *There is a canonical isomorphism*

$$(\bigwedge^n(E))^* \cong \bigwedge^n(E^*).$$

There is also a canonical isomorphism

$$\mu\colon \bigwedge^n(E^*) \cong \mathrm{Alt}^n(E; K)$$

which allows us to interpret alternating tensors over E^* as alternating multilinear maps.

Proof. The second isomorphism follows from the canonical isomorphism $(\bigwedge^n(E))^* \cong \bigwedge^n(E^*)$ and the canonical isomorphism $(\bigwedge^n(E))^* \cong \mathrm{Alt}^n(E;K)$ given by Proposition 34.5. □

Remarks:

1. The isomorphism $\mu\colon \bigwedge^n(E^*) \cong \mathrm{Alt}^n(E;K)$ discussed above can be described explicitly as the linear extension of the map given by

$$\mu(v_1^* \wedge \cdots \wedge v_n^*)(u_1, \ldots, u_n) = \det(v_j^*(u_i)).$$

2. The canonical isomorphism of Proposition 34.10 holds under more general conditions. Namely, that K is a commutative ring with identity and that E is a finitely-generated projective K-module (see Definition 35.7). See Bourbaki, [25] (Chapter III, §11, Section 5, Proposition 7).

3. Variants of our isomorphism μ are found in the literature. For example, there is a version μ', where

$$\mu' = \frac{1}{n!}\mu,$$

with the factor $\frac{1}{n!}$ added in front of the determinant. Each version has its its own merits and inconveniences. Morita [127] uses μ' because it is more convenient than μ when dealing with characteristic classes. On the other hand, μ' may not be defined for a field with positive characteristic, and when using μ', some extra factor is needed in defining the wedge operation of alternating multilinear forms (see Section 34.5) and for exterior differentiation. The version μ is the one adopted by Warner [184], Knapp [103], Fulton and Harris [69], and Cartan [34, 35].

If $f\colon E \to F$ is any linear map, by transposition we get a linear map $f^\top\colon F^* \to E^*$ given by

$$f^\top(v^*) = v^* \circ f, \qquad v^* \in F^*.$$

Consequently, we have

$$f^\top(v^*)(u) = v^*(f(u)), \qquad \text{for all } u \in E \text{ and all } v^* \in F^*.$$

For any $p \geq 1$, the map

$$(u_1, \ldots, u_p) \mapsto f(u_1) \wedge \cdots \wedge f(u_p)$$

from E^p to $\bigwedge^p F$ is multilinear alternating, so it induces a unique linear map $\bigwedge^p f\colon \bigwedge^p E \to \bigwedge^p F$ making the following diagram commute

$$\begin{tikzcd}
E^p \arrow[r, "\iota_\wedge"] \arrow[dr] & \bigwedge^p E \arrow[d, "\bigwedge^p f"] \\
& \bigwedge^p F,
\end{tikzcd}$$

and defined on generators by

$$\Big(\bigwedge^p f\Big)(u_1 \wedge \cdots \wedge u_p) = f(u_1) \wedge \cdots \wedge f(u_p).$$

Combining $\bigwedge^p$ and duality, we get a linear map $\bigwedge^p f^\top\colon \bigwedge^p F^* \to \bigwedge^p E^*$ defined on generators by

$$\Big(\bigwedge^p f^\top\Big)(v_1^* \wedge \cdots \wedge v_p^*) = f^\top(v_1^*) \wedge \cdots \wedge f^\top(v_p^*).$$

Proposition 34.11. *If $f\colon E \to F$ is any linear map between two finite-dimensional vector spaces E and F, then*

$$\mu\Big(\Big(\bigwedge^p f^\top\Big)(\omega)\Big)(u_1, \ldots, u_p) = \mu(\omega)(f(u_1), \ldots, f(u_p)), \qquad \omega \in \bigwedge^p F^*,\ u_1, \ldots, u_p \in E.$$

Proof. It is enough to prove the formula on generators. By definition of μ, we have

$$\begin{aligned} \mu\Big(\Big(\bigwedge^p f^\top\Big)(v_1^* \wedge \cdots \wedge v_p^*)\Big)(u_1, \ldots, u_p) &= \mu(f^\top(v_1^*) \wedge \cdots \wedge f^\top(v_p^*))(u_1, \ldots, u_p) \\ &= \det(f^\top(v_j^*)(u_i)) \\ &= \det(v_j^*(f(u_i))) \\ &= \mu(v_1^* \wedge \cdots \wedge v_p^*)(f(u_1), \ldots, f(u_p)), \end{aligned}$$

as claimed. □

Remark: The map $\bigwedge^p f^\top$ is often denoted f^*, although this is an ambiguous notation since p is dropped. Proposition 34.11 gives us the behavior of $\bigwedge^p f^\top$ under the identification of $\bigwedge^p E^*$ and $\mathrm{Alt}^p(E; K)$ *via* the isomorphism μ.

As in the case of symmetric powers, the map from E^n to $\bigwedge^n(E)$ given by $(u_1, \ldots, u_n) \mapsto u_1 \wedge \cdots \wedge u_n$ yields a surjection $\pi\colon E^{\otimes n} \to \bigwedge^n(E)$. Now this map has some section, so there is some injection $\eta\colon \bigwedge^n(E) \to E^{\otimes n}$ with $\pi \circ \eta = \mathrm{id}$. As we saw in Proposition 34.10 there is a canonical isomorphism

$$(\bigwedge^n(E))^* \cong \bigwedge^n(E^*)$$

for any field K, even of positive characteristic. However, if our field K has characteristic 0, then there is a special section having a natural definition involving an antisymmetrization process.

Recall, from Section 33.10 that we have a left action of the symmetric group $\mathfrak{S}_n$ on $E^{\otimes n}$. The tensors $z \in E^{\otimes n}$ such that

$$\sigma \cdot z = \mathrm{sgn}(\sigma)\, z, \quad \text{for all} \quad \sigma \in \mathfrak{S}_n$$

are called *antisymmetrized* tensors. We define the map $\eta\colon E^n \to E^{\otimes n}$ by

$$\eta(u_1, \ldots, u_n) = \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} \mathrm{sgn}(\sigma)\, u_{\sigma(1)} \otimes \cdots \otimes u_{\sigma(n)}.$$[1]

[1] It is the division by $n!$ that requires the field to have characteristic zero.

As the right hand side is an alternating map, we get a unique linear map $\bigwedge^n \eta\colon \bigwedge^n(E) \to E^{\otimes n}$ making the following diagram commute.

$$\begin{tikzcd}
E^n \arrow[r, "\iota_\wedge"] \arrow[rd, "\eta"'] & \bigwedge^n(E) \arrow[d, "\bigwedge^n \eta"] \\
 & E^{\otimes n}.
\end{tikzcd}$$

Clearly, $\bigwedge^n \eta(\bigwedge^n(E))$ is the set of antisymmetrized tensors in $E^{\otimes n}$. If we consider the map $A = (\bigwedge^n \eta) \circ \pi\colon E^{\otimes n} \longrightarrow E^{\otimes n}$, it is easy to check that $A \circ A = A$. Therefore, A is a projection, and by linear algebra, we know that

$$E^{\otimes n} = A(E^{\otimes n}) \oplus \operatorname{Ker} A = \bigwedge^n \eta(\bigwedge^n(E)) \oplus \operatorname{Ker} A.$$

It turns out that $\operatorname{Ker} A = E^{\otimes n} \cap \mathfrak{I}_a = \text{Ker } \pi$, where $\mathfrak{I}_a$ is the two-sided ideal of $T(E)$ generated by all tensors of the form $u \otimes u \in E^{\otimes 2}$ (for example, see Knapp [103], Appendix A). Therefore, $\bigwedge^n \eta$ is injective,

$$E^{\otimes n} = \bigwedge^n \eta(\bigwedge^n(E)) \oplus (E^{\otimes n} \cap \mathfrak{I}_a) = \bigwedge^n \eta(\bigwedge^n(E)) \oplus \operatorname{Ker} \pi,$$

and the exterior tensor power $\bigwedge^n(E)$ is naturally embedded into $E^{\otimes n}$.

34.5 Exterior Algebras

As in the case of symmetric tensors, we can pack together all the exterior powers $\bigwedge^n(V)$ into an algebra.

Definition 34.5. Gieven any vector space V, the vector space

$$\bigwedge(V) = \bigoplus_{m \geq 0} \bigwedge^m(V)$$

is called the *exterior algebra (or Grassmann algebra) of* V.

To make $\bigwedge(V)$ into an algebra, we mimic the procedure used for symmetric powers. If $\mathfrak{I}_a$ is the two-sided ideal generated by all tensors of the form $u \otimes u \in V^{\otimes 2}$, we set

$$\bigwedge^{\bullet}(V) = T(V)/\mathfrak{I}_a.$$

Then $\bigwedge^{\bullet}(V)$ automatically inherits a multiplication operation, called *wedge product*, and since $T(V)$ is graded, that is

$$T(V) = \bigoplus_{m \geq 0} V^{\otimes m},$$

we have

$$\overset{\bullet}{\bigwedge}(V) = \bigoplus_{m\geq 0} V^{\otimes m}/(\mathfrak{I}_a \cap V^{\otimes m}).$$

However, it is easy to check that

$$\bigwedge^m(V) \cong V^{\otimes m}/(\mathfrak{I}_a \cap V^{\otimes m}),$$

so

$$\overset{\bullet}{\bigwedge}(V) \cong \bigwedge(V).$$

When V has finite dimension d, we actually have a finite direct sum (coproduct)

$$\bigwedge(V) = \bigoplus_{m=0}^{d} \bigwedge^m(V),$$

and since each $\bigwedge^m(V)$ has dimension $\binom{d}{m}$, we deduce that

$$\dim(\bigwedge(V)) = 2^d = 2^{\dim(V)}.$$

The multiplication, $\wedge\colon \bigwedge^m(V) \times \bigwedge^n(V) \to \bigwedge^{m+n}(V)$, is skew-symmetric in the following precise sense:

Proposition 34.12. *For all $\alpha \in \bigwedge^m(V)$ and all $\beta \in \bigwedge^n(V)$, we have*

$$\beta \wedge \alpha = (-1)^{mn}\alpha \wedge \beta.$$

Proof. Since $v \wedge u = -u \wedge v$ for all $u, v \in V$, Proposition 34.12 follows by induction. □

Since $\alpha \wedge \alpha = 0$ for every *simple* (also called *decomposable*) tensor $\alpha = u_1 \wedge \cdots \wedge u_n$, it seems natural to infer that $\alpha \wedge \alpha = 0$ for *every* tensor $\alpha \in \bigwedge(V)$. If we consider the case where $\dim(V) \leq 3$, we can indeed prove the above assertion. However, if $\dim(V) \geq 4$, the above fact is generally false! For example, when $\dim(V) = 4$, if (u_1, u_2, u_3, u_4) is a basis for V, for $\alpha = u_1 \wedge u_2 + u_3 \wedge u_4$, we check that

$$\alpha \wedge \alpha = 2u_1 \wedge u_2 \wedge u_3 \wedge u_4,$$

which is nonzero. However, if $\alpha \in \bigwedge^m E$ with m odd, since m^2 is also odd, we have

$$\alpha \wedge \alpha = (-1)^{m^2}\alpha \wedge \alpha = -\alpha \wedge \alpha,$$

so indeed $\alpha \wedge \alpha = 0$ (if K is not a field of characteristic 2).

The above discussion suggests that it might be useful to know when an alternating tensor is simple (decomposable). We will show in Section 34.7 that for tensors $\alpha \in \bigwedge^2(V)$, $\alpha \wedge \alpha = 0$ iff α is simple.

A general criterion for decomposability can be given in terms of some operations known as *left hook* and *right hook* (also called *interior products*); see Section 34.7.

It is easy to see that $\bigwedge(V)$ satisfies the following universal mapping property.

Proposition 34.13. *Given any K-algebra A, for any linear map $f \colon V \to A$, if $(f(v))^2 = 0$ for all $v \in V$, then there is a unique K-algebra homomorphism $\overline{f} \colon \bigwedge(V) \to A$ so that*

$$f = \overline{f} \circ i,$$

as in the diagram below.

$$\begin{tikzcd}
V \arrow[r, "i"] \arrow[dr, "f"'] & \bigwedge(V) \arrow[d, "\overline{f}"] \\
& A
\end{tikzcd}$$

When E is finite-dimensional, recall the isomorphism $\mu \colon \bigwedge^n(E^*) \longrightarrow \mathrm{Alt}^n(E;K)$, defined as the linear extension of the map given by

$$\mu(v_1^* \wedge \cdots \wedge v_n^*)(u_1, \ldots, u_n) = \det(v_j^*(u_i)).$$

Now, we have also a multiplication operation $\bigwedge^m(E^*) \times \bigwedge^n(E^*) \longrightarrow \bigwedge^{m+n}(E^*)$. The following question then arises:

Can we define a multiplication $\mathrm{Alt}^m(E;K) \times \mathrm{Alt}^n(E;K) \longrightarrow \mathrm{Alt}^{m+n}(E;K)$ directly on alternating multilinear forms, so that the following diagram commutes?

$$\begin{tikzcd}
\bigwedge^m(E^*) \times \bigwedge^n(E^*) \arrow[r, "\wedge"] \arrow[d, "\mu_m \times \mu_n"] & \bigwedge^{m+n}(E^*) \arrow[d, "\mu_{m+n}"] \\
\mathrm{Alt}^m(E;K) \times \mathrm{Alt}^n(E;K) \arrow[r, "\wedge"] & \mathrm{Alt}^{m+n}(E;K)
\end{tikzcd}$$

As in the symmetric case, the answer is *yes*! The solution is to define this multiplication such that, for $f \in \mathrm{Alt}^m(E;K)$ and $g \in \mathrm{Alt}^n(E;K)$,

$$(f \wedge g)(u_1, \ldots, u_{m+n}) = \sum_{\sigma \in \mathrm{shuffle}(m,n)} \mathrm{sgn}(\sigma)\, f(u_{\sigma(1)}, \ldots, u_{\sigma(m)}) g(u_{\sigma(m+1)}, \ldots, u_{\sigma(m+n)}), \quad (**)$$

where shuffle(m, n) consists of all (m, n)-"shuffles;" that is, permutations σ of $\{1, \ldots m+n\}$ such that $\sigma(1) < \cdots < \sigma(m)$ and $\sigma(m+1) < \cdots < \sigma(m+n)$. For example, when $m = n = 1$, we have

$$(f \wedge g)(u, v) = f(u)g(v) - g(u)f(v).$$

When $m = 1$ and $n \geq 2$, check that

$$(f \wedge g)(u_1, \ldots, u_{m+1}) = \sum_{i=1}^{m+1} (-1)^{i-1} f(u_i) g(u_1, \ldots, \widehat{u_i}, \ldots, u_{m+1}),$$

where the hat over the argument u_i means that it should be omitted.

Here is another explicit example. Suppose $m = 2$ and $n = 1$. Given $v_1^*, v_2^*, v_3^* \in E^*$, the multiplication structure on $\bigwedge(E^*)$ implies that $(v_1^* \wedge v_2^*) \cdot v_3^* = v_1^* \wedge v_2^* \wedge v_3^* \in \bigwedge^3(E^*)$. Furthermore, for $u_1, u_2, u_3, \in E$,

$$\begin{aligned}
\mu_3(v_1^* \wedge v_2^* \wedge v_3^*)(u_1, u_2, u_3) &= \sum_{\sigma \in \mathfrak{S}_3} \mathrm{sgn}(\sigma) v_{\sigma(1)}^*(u_1) v_{\sigma(2)}^*(u_2) v_{\sigma(3)}^*(u_3) \\
&= v_1^*(u_1) v_2^*(u_2) v_3^*(u_3) - v_1^*(u_1) v_3^*(u_2) v_2^*(u_3) \\
&\quad - v_2^*(u_1) v_1^*(u_2) v_3^*(u_3) + v_2^*(u_1) v_3^*(u_2) v_1^*(u_3) \\
&\quad + v_3^*(u_1) v_1^*(u_2) v_2^*(u_3) - v_3^*(u_1) v_2^*(u_2) v_1^*(u_3).
\end{aligned}$$

Now the $(2, 1)$- shuffles of $\{1, 2, 3\}$ are the following three permutations, namely

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

If $f \cong \mu_2(v_1^* \wedge v_2^*)$ and $g \cong \mu_1(v_3^*)$, then $(**)$ implies that

$$\begin{aligned}
(f \cdot g)(u_1, u_2, u_3) &= \sum_{\sigma \in \mathrm{shuffle}(2,1)} \mathrm{sgn}(\sigma) f(u_{\sigma(1)}, u_{\sigma(2)}) g(u_{\sigma(3)}) \\
&= f(u_1, u_2) g(u_3) - f(u_1, u_3) g(u_2) + f(u_2, u_3) g(u_1) \\
&= \mu_2(v_1^* \wedge v_2^*)(u_1, u_2) \mu_1(v_3^*)(u_3) - \mu_2(v_1^* \wedge v_2^*)(u_1, u_3) \mu_1(v_3^*)(u_2) \\
&\quad + \mu_2(v_1^* \wedge v_2^*)(u_2, u_3) \mu_1(v_3^*)(u_1) \\
&= (v_1^*(u_1) v_2^*(u_2) - v_2^*(u_1) v_1^*(u_2)) v_3^*(u_3) \\
&\quad - (v_1^*(u_1) v_2^*(u_3) - v_2^*(u_1) v_1^*(u_3)) v_3^*(u_2) \\
&\quad + (v_1^*(u_2) v_2^*(u_3) - v_2^*(u_2) v_1^*(u_3)) v_3^*(u_1) \\
&= \mu_3(v_1^* \wedge v_2^* \wedge v_3^*)(u_1, u_2, u_3).
\end{aligned}$$

As a result of all this, the direct sum

$$\mathrm{Alt}(E) = \bigoplus_{n \geq 0} \mathrm{Alt}^n(E; K)$$

is an algebra under the above multiplication, and this algebra is isomorphic to $\bigwedge(E^*)$. For the record we state

Proposition 34.14. *When E is finite dimensional, the maps $\mu\colon \bigwedge^n(E^*) \longrightarrow \mathrm{Alt}^n(E;K)$ induced by the linear extensions of the maps given by*

$$\mu(v_1^* \wedge \cdots \wedge v_n^*)(u_1, \ldots, u_n) = \det(v_j^*(u_i))$$

yield a canonical isomorphism of algebras $\mu\colon \bigwedge(E^*) \longrightarrow \mathrm{Alt}(E)$, where the multiplication in $\mathrm{Alt}(E)$ is defined by the maps $\wedge\colon \mathrm{Alt}^m(E;K) \times \mathrm{Alt}^n(E;K) \longrightarrow \mathrm{Alt}^{m+n}(E;K)$, with

$$(f \wedge g)(u_1, \ldots, u_{m+n}) = \sum_{\sigma \in \mathrm{shuffle}(m,n)} \mathrm{sgn}(\sigma)\, f(u_{\sigma(1)}, \ldots, u_{\sigma(m)}) g(u_{\sigma(m+1)}, \ldots, u_{\sigma(m+n)}),$$

where shuffle(m, n) *consists of all (m, n)-"shuffles," that is, permutations σ of $\{1, \ldots m+n\}$ such that $\sigma(1) < \cdots < \sigma(m)$ and $\sigma(m+1) < \cdots < \sigma(m+n)$.*

Remark: The algebra $\bigwedge(E)$ is a graded algebra. Given two graded algebras E and F, we can make a new tensor product $E \mathbin{\widehat{\otimes}} F$, where $E \mathbin{\widehat{\otimes}} F$ is equal to $E \otimes F$ as a vector space, but with a skew-commutative multiplication given by

$$(a \otimes b) \wedge (c \otimes d) = (-1)^{\deg(b)\deg(c)}(ac) \otimes (bd),$$

where $a \in E^m, b \in F^p$, $c \in E^n, d \in F^q$. Then, it can be shown that

$$\bigwedge(E \oplus F) \cong \bigwedge(E) \mathbin{\widehat{\otimes}} \bigwedge(F).$$

34.6 The Hodge ∗-Operator

In order to define a generalization of the Laplacian that applies to differential forms on a Riemannian manifold, we need to define isomorphisms

$$\bigwedge^k V \longrightarrow \bigwedge^{n-k} V,$$

for any Euclidean vector space V of dimension n and any k, with $0 \leq k \leq n$. If $\langle -, - \rangle$ denotes the inner product on V, we define an inner product on $\bigwedge^k V$, denoted $\langle -, - \rangle_\wedge$, by setting

$$\langle u_1 \wedge \cdots \wedge u_k, v_1 \wedge \cdots \wedge v_k \rangle_\wedge = \det(\langle u_i, v_j \rangle),$$

for all $u_i, v_i \in V$, and extending $\langle -, - \rangle_\wedge$ by bilinearity.

It is easy to show that if $(e_1, \ldots, e_n)$ is an orthonormal basis of V, then the basis of $\bigwedge^k V$ consisting of the e_I (where $I = \{i_1, \ldots, i_k\}$, with $1 \leq i_1 < \cdots < i_k \leq n$) is an orthonormal basis of $\bigwedge^k V$. Since the inner product on V induces an inner product on V^* (recall that $\langle \omega_1, \omega_2 \rangle = \langle \omega_1^\sharp, \omega_2^\sharp \rangle$, for all $\omega_1, \omega_2 \in V^*$), we also get an inner product on $\bigwedge^k V^*$.

Definition 34.6. An *orientation* of a vector space V of dimension n is given by the choice of some basis $(e_1, \ldots, e_n)$. We say that a basis $(u_1, \ldots, u_n)$ of V is *positively oriented* iff $\det(u_1, \ldots, u_n) > 0$ (where $\det(u_1, \ldots, u_n)$ denotes the determinant of the matrix whose jth column consists of the coordinates of u_j over the basis $(e_1, \ldots, e_n)$), otherwise it is *negatively oriented*. An *oriented vector space* is a vector space V together with an orientation of V.

If V is oriented by the basis $(e_1, \ldots, e_n)$, then V^* is oriented by the dual basis $(e_1^*, \ldots, e_n^*)$. If σ is any permutation of $\{1, \ldots, n\}$, then the basis $(e_{\sigma(1)}, \ldots, e_{\sigma(n)})$ has positive orientation iff the signature $\mathrm{sgn}(\sigma)$ of the permutation σ is even.

If V is an oriented vector space of dimension n, then we can define a linear isomorphism

$$*\colon \bigwedge^k V \to \bigwedge^{n-k} V,$$

called the *Hodge $*$-operator*. The existence of this operator is guaranteed by the following proposition.

Proposition 34.15. *Let V be any oriented Euclidean vector space whose orientation is given by some chosen orthonormal basis $(e_1, \ldots, e_n)$. For any alternating tensor $\alpha \in \bigwedge^k V$, there is a unique alternating tensor $*\alpha \in \bigwedge^{n-k} V$ such that*

$$\alpha \wedge \beta = \langle *\alpha, \beta \rangle_\wedge \, e_1 \wedge \cdots \wedge e_n$$

for all $\beta \in \bigwedge^{n-k} V$. The alternating tensor $*\alpha$ is independent of the choice of the positive orthonormal basis $(e_1, \ldots, e_n)$.

Proof. Since $\bigwedge^n V$ has dimension 1, the alternating tensor $e_1 \wedge \cdots \wedge e_n$ is a basis of $\bigwedge^n V$. It follows that for any fixed $\alpha \in \bigwedge^k V$, the linear map λ_α from $\bigwedge^{n-k} V$ to $\bigwedge^n V$ given by

$$\lambda_\alpha(\beta) = \alpha \wedge \beta$$

is of the form

$$\lambda_\alpha(\beta) = f_\alpha(\beta) \, e_1 \wedge \cdots \wedge e_n$$

for some linear form $f_\alpha \in \left(\bigwedge^{n-k} V\right)^*$. But then, by the duality induced by the inner product $\langle -, - \rangle$ on $\bigwedge^{n-k} V$, there is a unique vector $*\alpha \in \bigwedge^{n-k} V$ such that

$$f_\lambda(\beta) = \langle *\alpha, \beta \rangle_\wedge \quad \text{for all } \beta \in \bigwedge^{n-k} V,$$

which implies that

$$\alpha \wedge \beta = \lambda_\alpha(\beta) = f_\alpha(\beta) \, e_1 \wedge \cdots \wedge e_n = \langle *\alpha, \beta \rangle_\wedge \, e_1 \wedge \cdots \wedge e_n,$$

as claimed. If $(e'_1, \ldots, e'_n)$ is any other positively oriented orthonormal basis, by Proposition 34.2, $e'_1 \wedge \cdots \wedge e'_n = \det(P) \, e_1 \wedge \cdots \wedge e_n = e_1 \wedge \cdots \wedge e_n$, since $\det(P) = 1$ where P is the change of basis from $(e_1, \ldots, e_n)$ to $(e'_1, \ldots, e'_n)$ and both bases are positively oriented. □

Definition 34.7. The operator $*$ from $\bigwedge^k V$ to $\bigwedge^{n-k} V$ defined by Proposition 34.15 is called the *Hodge $*$-operator*.

Obseve that the Hodge $*$-operator is linear.

The Hodge $*$-operator is defined in terms of the orthonormal basis elements of $\bigwedge V$ as follows: For any increasing sequence $(i_1, \ldots, i_k)$ of elements $i_p \in \{1, \ldots, n\}$, if $(j_1, \ldots, j_{n-k})$ is the increasing sequence of elements $j_q \in \{1, \ldots, n\}$ such that

$$\{i_1, \ldots, i_k\} \cup \{j_1, \ldots, j_{n-k}\} = \{1, \ldots, n\},$$

then

$$*(e_{i_1} \wedge \cdots \wedge e_{i_k}) = \mathrm{sign}(i_1, \ldots i_k, j_1, \ldots, j_{n-k})\, e_{j_1} \wedge \cdots \wedge e_{j_{n-k}}.$$

In particular, for $k = 0$ and $k = n$, we have

$$\begin{aligned} *(1) &= e_1 \wedge \cdots \wedge e_n \\ *(e_1 \wedge \cdots \wedge e_n) &= 1. \end{aligned}$$

For example, if $n = 3$, we have

$$\begin{aligned} *e_1 &= e_2 \wedge e_3 \\ *e_2 &= -e_1 \wedge e_3 \\ *e_3 &= e_1 \wedge e_2 \\ *(e_1 \wedge e_2) &= e_3 \\ *(e_1 \wedge e_3) &= -e_2 \\ *(e_2 \wedge e_3) &= e_1. \end{aligned}$$

The Hodge $*$-operators $*\colon \bigwedge^k V \to \bigwedge^{n-k} V$ induce a linear map $*\colon \bigwedge(V) \to \bigwedge(V)$. We also have Hodge $*$-operators $*\colon \bigwedge^k V^* \to \bigwedge^{n-k} V^*$.

The following proposition shows that the linear map $*\colon \bigwedge(V) \to \bigwedge(V)$ is an isomorphism.

Proposition 34.16. *If V is any oriented vector space of dimension n, for every k with $0 \leq k \leq n$, we have*

(i) $** = (-\mathrm{id})^{k(n-k)}$.

(ii) $\langle x, y \rangle_{\wedge} = *(x \wedge *y) = *(y \wedge *x)$, *for all* $x, y \in \bigwedge^k V$.

Proof. (1) Let $(e_i)_{i=1}^n$ is an orthonormal basis of V. It is enough to check the identity on basis elements. We have

$$*(e_{i_1} \wedge \cdots \wedge e_{i_k}) = \mathrm{sign}(i_1, \ldots i_k, j_1, \ldots, j_{n-k})\, e_{j_1} \wedge \cdots \wedge e_{j_{n-k}}$$

and

$$\begin{aligned}**(e_{i_1}\wedge\cdots\wedge e_{i_k}) &= \mathrm{sign}(i_1,\ldots i_k,j_1,\ldots,j_{n-k})\ *(e_{j_1}\wedge\cdots\wedge e_{j_{n-k}})\\ &= \mathrm{sign}(i_1,\ldots i_k,j_1,\ldots,j_{n-k})\,\mathrm{sign}(j_1,\ldots,j_{n-k},i_1,\ldots i_k)\,e_{i_1}\wedge\cdots\wedge e_{i_k}.\end{aligned}$$

It is easy to see that

$$\mathrm{sign}(i_1,\ldots i_k,j_1,\ldots,j_{n-k})\,\mathrm{sign}(j_1,\ldots,j_{n-k},i_1,\ldots i_k)\ = (-1)^{k(n-k)},$$

which yields

$$**(e_{i_1}\wedge\cdots\wedge e_{i_k}) = (-1)^{k(n-k)}\,e_{i_1}\wedge\cdots\wedge e_{i_k},$$

as claimed.

(ii) These identities are easily checked on basis elements; see Jost [99], Chapter 2, Lemma 2.1.1. In particular let

$$x = e_{i_1}\wedge\cdots\wedge e_{i_k},\qquad y = e_{i_j}\wedge\cdots\wedge e_{i_j},\qquad x,y\in\bigwedge^k V,$$

where $(e_i)_{i=1}^n$ is an orthonormal basis of V. If $x\neq y$, $\langle x,y\rangle_\wedge = 0$ since there is some e_{i_p} of x not equal to any e_{j_q} of y by the orthonormality of the basis, this means the p^{th} row of $(\langle e_{i_l},e_{j_s}\rangle)$ consists entirely of zeroes. Also $x\neq y$ implies that $y\wedge *x = 0$ since

$$*x = \mathrm{sign}(i_1,\ldots i_k,l_1,\ldots,l_{n-k})e_{l_1}\wedge\cdots\wedge e_{l_{n-k}},$$

where e_{l_s} is the same as some e_p in y. A similar argument shows that if $x\neq y$, $x\wedge *y = 0$. So now assume $x = y$. Then

$$\begin{aligned}*(e_{i_1}\wedge\cdots\wedge e_{i_k}\wedge *(e_{i_1}\wedge\cdots\wedge e_{i_k})) &= *(e_1\wedge e_2\cdots\wedge e_n)\\ &= 1 = \langle x,x\rangle_\wedge.\end{aligned}$$ □

It is possible to express $*(1)$ in terms of any basis (not necessarily orthonormal) of V.

Proposition 34.17. *If V is any finite-dimensional oriented vector space, for any basis $(v_!,\ldots,v_n)$ of V, we have*

$$*(1) = \frac{1}{\sqrt{\det(\langle v_i,v_j\rangle)}}\,v_1\wedge\cdots\wedge v_n.$$

Proof. If $(e_1,\ldots,e_n)$ is an orthonormal basis of V and $(v_1,\ldots,v_n)$ is any other basis of V, then

$$\langle v_1\wedge\cdots\wedge v_n, v_1\wedge\cdots\wedge v_n\rangle_\wedge = \det(\langle v_i,v_j\rangle),$$

and since

$$v_1\wedge\cdots\wedge v_n = \det(A)\,e_1\wedge\cdots\wedge e_n$$

where A is the matrix expressing the v_j in terms of the e_i, we have

$$\langle v_1 \wedge \cdots \wedge v_n, v_1 \wedge \cdots \wedge v_n \rangle_\wedge = \det(A)^2 \langle e_1 \wedge \cdots \wedge e_n, e_1 \wedge \cdots \wedge e_n \rangle = \det(A)^2.$$

As a consequence, $\det(A) = \sqrt{\det(\langle v_i, v_j \rangle)}$, and

$$v_1 \wedge \cdots \wedge v_n = \sqrt{\det(\langle v_i, v_j \rangle)}\, e_1 \wedge \cdots \wedge e_n,$$

from which it follows that

$$*(1) = \frac{1}{\sqrt{\det(\langle v_i, v_j \rangle)}}\, v_1 \wedge \cdots \wedge v_n$$

(see Jost [99], Chapter 2, Lemma 2.1.3). □

34.7 Left and Right Hooks ⊛

In this section *all vector spaces are assumed to have finite dimension*. Say $\dim(E) = n$. Using our nonsingular pairing

$$\langle -, - \rangle \colon \bigwedge^p E^* \times \bigwedge^p E \longrightarrow K \qquad (1 \leq p \leq n)$$

defined on generators by

$$\langle u_1^* \wedge \cdots \wedge u_p^*, v_1 \wedge \cdots \wedge u_p \rangle = \det(u_i^*(v_j)),$$

we define various contraction operations (partial evaluation operators)

$$\lrcorner \colon \bigwedge^p E \times \bigwedge^{p+q} E^* \longrightarrow \bigwedge^q E^* \qquad \text{(left hook)}$$

and

$$\llcorner \colon \bigwedge^{p+q} E^* \times \bigwedge^p E \longrightarrow \bigwedge^q E^* \qquad \text{(right hook)},$$

as well as the versions obtained by replacing E by E^* and E^{**} by E. We begin with the *left interior product or left hook,* $\lrcorner$.

Let $u \in \bigwedge^p E$. For any q such that $p + q \leq n$, multiplication on the right by u is a linear map

$$\wedge_R(u) \colon \bigwedge^q E \longrightarrow \bigwedge^{p+q} E$$

given by

$$v \mapsto v \wedge u$$

where $v \in \bigwedge^q E$. The transpose of $\wedge_R(u)$ yields a linear map

$$(\wedge_R(u))^\top\colon \Big(\bigwedge^{p+q} E\Big)^* \longrightarrow \Big(\bigwedge^{q} E\Big)^*,$$

which, using the isomorphisms $\left(\bigwedge^{p+q} E\right)^* \cong \bigwedge^{p+q} E^*$ and $\left(\bigwedge^{q} E\right)^* \cong \bigwedge^{q} E^*$, can be viewed as a map

$$(\wedge_R(u))^\top\colon \bigwedge^{p+q} E^* \longrightarrow \bigwedge^{q} E^*$$

given by

$$z^* \mapsto z^* \circ \wedge_R(u),$$

where $z^* \in \bigwedge^{p+q} E^*$. We denote $z^* \circ \wedge_R(u)$ by $u \lrcorner\, z^*$. In terms of our pairing, the adjoint $u \lrcorner$ of $\wedge_R(u)$ defined by

$$\langle u \lrcorner\, z^*, v\rangle = \langle z^*, \wedge_R(u)(v)\rangle;$$

this in turn leads to the following definition.

Definition 34.8. Let $u \in \bigwedge^p E$ and $z^* \in \bigwedge^{p+q} E^*$. We define $u \lrcorner\, z^* \in \bigwedge^q E^*$ to be q-vector uniquely determined by

$$\langle u \lrcorner\, z^*, v\rangle = \langle z^*, v \wedge u\rangle, \quad \text{for all } v \in \bigwedge^q E.$$

Remark: Note that to be precise the operator

$$\lrcorner\,\colon \bigwedge^p E \times \bigwedge^{p+q} E^* \longrightarrow \bigwedge^{q} E^*$$

depends of p, q, so we really defined a family of operators $\lrcorner_{\,p,q}$. This family of operators $\lrcorner_{\,p,q}$ induces a map

$$\lrcorner\,\colon \bigwedge E \times \bigwedge E^* \longrightarrow \bigwedge E^*,$$

with

$$\lrcorner_{\,p,q}\colon \bigwedge^p E \times \bigwedge^{p+q} E^* \longrightarrow \bigwedge^{q} E^*$$

as defined before. The common practice is to omit the subscripts of $\lrcorner$.

It is immediately verified that

$$(u \wedge v) \lrcorner\, z^* = u \lrcorner\, (v \lrcorner\, z^*),$$

for all $u \in \bigwedge^k E, v \in \bigwedge^{p-k} E$, $z^* \in \bigwedge^{p+q} E^*$ since

$$\langle (u \wedge v) \lrcorner\, z^*, w\rangle = \langle z^*, w \wedge u \wedge v\rangle = \langle v \lrcorner\, z^*, w \wedge u\rangle = \langle u \lrcorner\, (v \lrcorner\, z^*), w\rangle,$$

whenever $w \in \bigwedge^q E$. This means that

$$\lrcorner : \bigwedge E \times \bigwedge E^* \longrightarrow \bigwedge E^*$$

is a left action of the (noncommutative) ring $\bigwedge E$ with multiplication $\wedge$ on $\bigwedge E^*$, which makes $\bigwedge E^*$ into a left $\bigwedge E$-module.

By interchanging E and E^* and using the isomorphism

$$\left(\bigwedge^k F\right)^* \cong \bigwedge^k F^*,$$

we can also define some maps

$$\lrcorner : \bigwedge^p E^* \times \bigwedge^{p+q} E \longrightarrow \bigwedge^q E,$$

and make the following definition.

Definition 34.9. Let $u^* \in \bigwedge^p E^*$, and $z \in \bigwedge^{p+q} E$. We define $u^* \lrcorner\, z \in \bigwedge^q$ as the q-vector uniquely defined by

$$\langle v^* \wedge u^*, z\rangle = \langle v^*, u^* \lrcorner\, z\rangle, \quad \text{for all } v^* \in \bigwedge^q E^*.$$

As for the previous version, we have a family of operators $\lrcorner_{p,q}$ which define an operator

$$\lrcorner : \bigwedge E^* \times \bigwedge E \longrightarrow \bigwedge E.$$

We easily verify that

$$(u^* \wedge v^*) \lrcorner\, z = u^* \lrcorner\, (v^* \lrcorner\, z),$$

whenever $u^* \in \bigwedge^k E^*$, $v^* \in \bigwedge^{p-k} E^*$, and $z \in \bigwedge^{p+q} E$; so this version of $\lrcorner$ is a left action of the ring $\bigwedge E^*$ on $\bigwedge E$ which makes $\bigwedge E$ into a left $\bigwedge E^*$-module.

In order to proceed any further we need some combinatorial properties of the basis of $\bigwedge^p E$ constructed from a basis $(e_1, \ldots, e_n)$ of E. Recall that for any (nonempty) subset $I \subseteq \{1, \ldots, n\}$, we let

$$e_I = e_{i_1} \wedge \cdots \wedge e_{i_p},$$

where $I = \{i_1, \ldots, i_p\}$ with $i_1 < \cdots < i_p$. We also let $e_\emptyset = 1$.

Given any two nonempty subsets $H, L \subseteq \{1, \ldots, n\}$ both listed in increasing order, say $H = \{h_1 < \ldots < h_p\}$ and $L = \{\ell_1 < \ldots < \ell_q\}$, if H and L are disjoint, let $H \cup L$ be union of H and L considered as the ordered sequence

$$(h_1, \ldots, h_p, \ell_1, \ldots, \ell_q).$$

Then let

$$\rho_{H,L} = \begin{cases} 0 & \text{if } H \cap L \neq \emptyset, \\ (-1)^\nu & \text{if } H \cap L = \emptyset, \end{cases}$$

where

$$\nu = |\{(h, l) \mid (h, l) \in H \times L,\, h > l\}|.$$

Observe that when $H \cap L = \emptyset$, $|H| = p$ and $|L| = q$, the number ν is the number of inversions of the sequence

$$(h_1, \cdots, h_p, \ell_1, \cdots, \ell_q),$$

where an inversion is a pair (h_i, ℓ_j) such that $h_i > \ell_j$.

Unless $p + q = n$, the function whose graph is given by

$$\begin{pmatrix} 1 & \cdots & p & p+1 & \cdots & p+q \\ h_1 & \cdots & h_p & \ell_1 & \cdots & \ell_q \end{pmatrix}$$

is **not** a permutation of $\{1, \ldots, n\}$. We can view ν as a slight generalization of the notion of the number of inversions of a permutation.

Proposition 34.18. *For any basis $(e_1, \ldots, e_n)$ of E the following properties hold:*

(1) If $H \cap L = \emptyset$, $|H| = p$, and $|L| = q$, then

$$\rho_{H,L}\rho_{L,H} = (-1)^{\nu}(-1)^{pq-\nu} = (-1)^{pq}.$$

(2) For $H, L \subseteq \{1, \ldots, m\}$ listed in increasing order, we have

$$e_H \wedge e_L = \rho_{H,L} e_{H \cup L}.$$

Similarly,

$$e^*_H \wedge e^*_L = \rho_{H,L} e^*_{H \cup L}.$$

(3) For the left hook

$$\lrcorner\colon \bigwedge^p E \times \bigwedge^{p+q} E^* \longrightarrow \bigwedge^q E^*,$$

we have

$$\begin{aligned} e_H \lrcorner\, e^*_L &= 0 \quad \textit{if } H \not\subseteq L \\ e_H \lrcorner\, e^*_L &= \rho_{L-H,H} e^*_{L-H} \quad \textit{if } H \subseteq L. \end{aligned}$$

(4) For the left hook

$$\lrcorner\colon \bigwedge^p E^* \times \bigwedge^{p+q} E \longrightarrow \bigwedge^q E,$$

we have

$$\begin{aligned} e^*_H \lrcorner\, e_L &= 0 \quad \textit{if } H \not\subseteq L \\ e^*_H \lrcorner\, e_L &= \rho_{L-H,H} e_{L-H} \quad \textit{if } H \subseteq L. \end{aligned}$$

Proof. These are proved in Bourbaki [25] (Chapter III, §11, Section 11), but the proofs of (3) and (4) are very concise. We elaborate on the proofs of (2) and (4), the proof of (3) being similar.

In (2) if $H \cap L \neq \emptyset$, then $e_H \wedge e_L$ contains some vector twice and so $e_H \wedge e_L = 0$. Otherwise, $e_H \wedge e_L$ consists of

$$e_{h_1} \wedge \cdots \wedge e_{h_p} \wedge e_{\ell_1} \wedge \cdots \wedge e_{\ell_q},$$

and to order the sequence of indices in increasing order we need to transpose any two indices (h_i, ℓ_j) corresponding to an inversion, which yields $\rho_{H,L} e_{H \cup L}$.

Let us now consider (4). We have $|L| = p + q$ and $|H| = p$, and the q-vector $e_H^* \lrcorner e_L$ is characterized by

$$\langle v^*, e_H^* \lrcorner e_L \rangle = \langle v^* \wedge e_H^*, e_L \rangle$$

for all $v^* \in \bigwedge^q E^*$. There are two cases.

Case 1: $H \not\subseteq L$. If so, no matter what $v^* \in \bigwedge^q E^*$ is, since H contains some index h not in L, the hth row $(e_h^*(e_{\ell_1}), \ldots, e_h^*(e_{\ell_{p+q}}))$ of the determinant $\langle v^* \wedge e_H^*, e_L \rangle$ must be zero, so $\langle v^* \wedge e_H^*, e_L \rangle = 0$ for all $v^* \in \bigwedge^q E^*$, and since the pairing is nongenerate, we must have $e_H^* \lrcorner e_L = 0$.

Case 2: $H \subseteq L$. In this case, for $v^* = e_{L-H}^*$, by (2) we have

$$\langle e_{L-H}^*, e_H^* \lrcorner e_L \rangle = \langle e_{L-H}^* \wedge e_H^*, e_L \rangle = \langle \rho_{L-H,H} e_L^*, e_L \rangle = \rho_{L-H,H},$$

which yields

$$\langle e_{L-H}^*, e_H^* \lrcorner e_L \rangle = \rho_{L-H,H}.$$

The q-vector $e_H^* \lrcorner e_L$ can be written as a linear combination $e_H^* \lrcorner e_L = \sum_J \lambda_J e_J$ with $|J| = q$ so

$$\langle e_{L-H}^*, e_H^* \lrcorner e_L \rangle = \sum_J \lambda_J \langle e_{L-H}^*, e_J \rangle.$$

By definition of the pairing, $\langle e_{L-H}^*, e_J \rangle = 0$ unless $J = L - H$, which means that

$$\langle e_{L-H}^*, e_H^* \lrcorner e_L \rangle = \lambda_{L-H} \langle e_{L-H}^*, e_{L-H} \rangle = \lambda_{L-H},$$

so $\lambda_{L-H} = \rho_{L-H,H}$, as claimed. □

Using Proposition 34.18, we have the

Proposition 34.19. *For the left hook*

$$\lrcorner : E \times \bigwedge^{q+1} E^* \longrightarrow \bigwedge^{q} E^*,$$

for every $u \in E$, $x^* \in \bigwedge^{q+1-s} E^*$, and $y^* \in \bigwedge^s E^*$, we have

$$u \lrcorner (x^* \wedge y^*) = (-1)^s (u \lrcorner x^*) \wedge y^* + x^* \wedge (u \lrcorner y^*).$$

Proof. We can prove the above identity assuming that x^* and y^* are of the form e_I^* and e_J^* using Proposition 34.18 and leave the details as an exercise for the reader. $\square$

Thus, $\lrcorner : E \times \bigwedge^{q+1} E^* \longrightarrow \bigwedge^q E^*$ is almost an anti-derivation, except that the sign $(-1)^s$ is applied to the wrong factor.

We have a similar identity for the other version of the left hook

$$\lrcorner : E^* \times \bigwedge^{q+1} E \longrightarrow \bigwedge^{q} E,$$

namely

$$u^* \lrcorner (x \wedge y) = (-1)^s (u^* \lrcorner x) \wedge y + x \wedge (u^* \lrcorner y)$$

for every $u^* \in E^*$, $x \in \bigwedge^{q+1-s} E$, and $y \in \bigwedge^s E$.

An application of this formula when $q = 3$ and $s = 2$ yields an interesting equation. In this case, $u^* \in E^*$ and $x, y \in \bigwedge^2 E$, so we get

$$u^* \lrcorner (x \wedge y) = (u^* \lrcorner x) \wedge y + x \wedge (u^* \lrcorner y).$$

In particular, for $x = y$, since $x \in \bigwedge^2 E$ and $u^* \lrcorner x \in E$, Proposition 34.12 implies that $(u^* \lrcorner x) \wedge x = x \wedge (u^* \lrcorner x)$, and we obtain

$$u^* \lrcorner (x \wedge x) = 2((u^* \lrcorner x) \wedge x). \tag{$\dagger$}$$

As a consequence, $(u^* \lrcorner x) \wedge x = 0$ iff $u^* \lrcorner (x \wedge x) = 0$. We will use this identity together with Proposition 34.25 to prove that a 2-vector $x \in \bigwedge^2 E$ is decomposable iff $x \wedge x = 0$.

It is also possible to define a *right interior product or right hook* $\llcorner$, using multiplication on the left rather than multiplication on the right. Then we use the maps

$$\llcorner : \bigwedge^{p+q} E^* \times \bigwedge^{p} E \longrightarrow \bigwedge^{q} E^*$$

to make the following definition.

Definition 34.10. Let $u \in \bigwedge^p E$ and $z^* \in \bigwedge^{p+q} E^*$. We define $z^* \llcorner u \in \bigwedge^q E^*$ to be the q-vector uniquely defined as

$$\langle z^* \llcorner u, v \rangle = \langle z^*, u \wedge v \rangle, \qquad \text{for all } v \in \bigwedge^q E.$$

This time we can prove that

$$z^* \llcorner (u \wedge v) = (z^* \llcorner u) \llcorner v,$$

so the family of operators $\llcorner_{p,q}$ defines a right action

$$\llcorner : \bigwedge E^* \times \bigwedge E \longrightarrow \bigwedge E^*$$

of the ring $\bigwedge E$ on $\bigwedge E^*$ which makes $\bigwedge E^*$ into a right $\bigwedge E$-module.

Similarly, we have maps

$$\llcorner : \bigwedge^{p+q} E \times \bigwedge^{p} E^* \longrightarrow \bigwedge^{q} E$$

which in turn leads to the following dual formation of the right hook.

Definition 34.11. Let $u^* \in \bigwedge^p E^*$ and $z \in \bigwedge^{p+q} E$. We define $z \llcorner u^* \in \bigwedge^q$ to be the q-vector uniquely defined by

$$\langle u^* \wedge v^*, z\rangle = \langle v^*, z \llcorner u^*\rangle, \qquad \text{for all } v^* \in \bigwedge^q E^*.$$

We can prove that

$$z \llcorner (u^* \wedge v^*) = (z \llcorner u^*) \llcorner v^*,$$

so the family of operators $\llcorner_{p,q}$ defines a right action

$$\llcorner : \bigwedge E \times \bigwedge E^* \longrightarrow \bigwedge E$$

of the ring $\bigwedge E^*$ on $\bigwedge E$ which makes $\bigwedge E$ into a right $\bigwedge E^*$-module.

Since the left hook $\lrcorner : \bigwedge^p E \times \bigwedge^{p+q} E^* \longrightarrow \bigwedge^q E^*$ is defined by

$$\langle u \lrcorner z^*, v\rangle = \langle z^*, v \wedge u\rangle, \quad \text{for all } u \in \bigwedge^p E,\ v \in \bigwedge^q E \text{ and } z^* \in \bigwedge^{p+q} E^*,$$

the right hook

$$\llcorner : \bigwedge^{p+q} E^* \times \bigwedge^{p} E \longrightarrow \bigwedge^{q} E^*$$

by

$$\langle z^* \llcorner u, v\rangle = \langle z^*, u \wedge v\rangle, \quad \text{for all } u \in \bigwedge^p E,\ v \in \bigwedge^q E, \text{ and } z^* \in \bigwedge^{p+q} E^*,$$

and $v \wedge u = (-1)^{pq} u \wedge v$, we conclude that

$$z^* \llcorner u = (-1)^{pq}\, u \lrcorner z^*.$$

Similarly, since

$$\begin{aligned}
\langle v^* \wedge u^*, z\rangle &= \langle v^*, u^* \lrcorner z\rangle, \quad \text{for all } u^* \in \bigwedge^p E^*,\ v^* \in \bigwedge^q E^* \text{ and } z \in \bigwedge^{p+q} E\\
\langle u^* \wedge v^*, z\rangle &= \langle v^*, z \llcorner u^*\rangle, \quad \text{for all } u^* \in \bigwedge^p E^*,\ v^* \in \bigwedge^q E^*, \text{ and } z \in \bigwedge^{p+q} E,
\end{aligned}$$

and $v^* \wedge u^* = (-1)^{pq} u^* \wedge v^*$, we have

$$z \llcorner u^* = (-1)^{pq}\, u^* \lrcorner z.$$

We summarize the above facts in the following proposition.

Proposition 34.20. *The following identities hold:*

$$\begin{aligned} z^* \llcorner u &= (-1)^{pq}\, u \lrcorner z^* \quad \textit{for all } u \in \textstyle\bigwedge^p E \textit{ and all } z^* \in \textstyle\bigwedge^{p+q} E^* \\ z \llcorner u^* &= (-1)^{pq}\, u^* \lrcorner z \quad \textit{for all } u^* \in \textstyle\bigwedge^p E^* \textit{ and all } z \in \textstyle\bigwedge^{p+q} E. \end{aligned}$$

Therefore the left and right hooks are not independent, and in fact each one determines the other. As a consequence, we can restrict our attention to only one of the hooks, for example the left hook, but there are a few situations where it is nice to use both, for example in Proposition 34.23.

A version of Proposition 34.18 holds for right hooks, but beware that the indices in $\rho_{L-H,H}$ are permuted. This permutation has to do with the fact that the left hook and the right hook are related *via* a sign factor.

Proposition 34.21. *For any basis $(e_1, \ldots, e_n)$ of E the following properties hold:*

(1) For the right hook

$$\llcorner \colon \bigwedge^{p+q} E \times \bigwedge^{p} E^* \longrightarrow \bigwedge^{q} E$$

we have

$$\begin{aligned} e_L \llcorner e_H^* &= 0 \quad \textit{if } H \not\subseteq L \\ e_L \llcorner e_H^* &= \rho_{H,L-H} e_{L-H} \quad \textit{if } H \subseteq L. \end{aligned}$$

(2) For the right hook

$$\llcorner \colon \bigwedge^{p+q} E^* \times \bigwedge^{p} E \longrightarrow \bigwedge^{q} E^*$$

we have

$$\begin{aligned} e_L^* \llcorner e_H &= 0 \quad \textit{if } H \not\subseteq L \\ e_L^* \llcorner e_H &= \rho_{H,L-H} e_{L-H}^* \quad \textit{if } H \subseteq L. \end{aligned}$$

Remark: Our definition of left hooks as left actions $\lrcorner \colon \bigwedge^p E \times \bigwedge^{p+q} E^* \longrightarrow \bigwedge^q E^*$ and $\lrcorner \colon \bigwedge^p E^* \times \bigwedge^{p+q} E \longrightarrow \bigwedge^q E$ and right hooks as right actions $\llcorner \colon \bigwedge^{p+q} E^* \times \bigwedge^p E \longrightarrow \bigwedge^q E^*$ and $\llcorner \colon \bigwedge^{p+q} E \times \bigwedge^p E^* \longrightarrow \bigwedge^q E$ is identical to the definition found in Fulton and Harris [69] (Appendix B). However, the reader should be aware that this is not a universally accepted notation. In fact, the left hook $u^* \lrcorner z$ defined in Bourbaki [25] is our right hook $z \llcorner u^*$, up to the sign $(-1)^{p(p-1)/2}$. This has to do with the fact that Bourbaki uses a different pairing which also involves an extra sign, namely

$$\langle v^*, u^* \lrcorner z \rangle = (-1)^{p(p-1)/2} \langle u^* \wedge v^*, z \rangle.$$

One of the side-effects of this choice is that Bourbaki's version of Formula (4) of Proposition 34.18 (Bourbaki [25], Chapter III, page 168) is

$$\begin{aligned} e_H^* \lrcorner e_L &= 0 \quad \text{if } H \not\subseteq L \\ e_H^* \lrcorner e_L &= (-1)^{p(p-1)/2} \rho_{H,L-H} e_{L-H} \quad \text{if } H \subseteq L, \end{aligned}$$

where $|H| = p$ and $|L| = p + q$. This correspond to Formula (1) of Proposition 34.21 up to the sign factor $(-1)^{p(p-1)/2}$, which we find horribly confusing. Curiously, an older edition of Bourbaki (1958) uses the same pairing as Fulton and Harris [69]. The reason (and the advantage) for this change of sign convention is not clear to us.

We also have the following version of Proposition 34.19 for the right hook.

Proposition 34.22. *For the right hook*

$$\llcorner : \bigwedge^{q+1} E^* \times E \longrightarrow \bigwedge^{q} E^*,$$

for every $u \in E$, $x^* \in \bigwedge^r E^*$, and $y^* \in \bigwedge^{q+1-r} E^*$, we have

$$(x^* \wedge y^*) \llcorner u = (x^* \llcorner u) \wedge y^* + (-1)^r x^* \wedge (y^* \llcorner u).$$

Proof. A proof involving determinants can be found in Warner [184], Chapter 2. □

Thus, $\llcorner : \bigwedge^{q+1} E^* \times E \longrightarrow \bigwedge^q E^*$ is an anti-derivation. A similar formula holds for the the right hook $\llcorner : \bigwedge^{q+1} E \times E^* \longrightarrow \bigwedge^q E$, namely

$$(x \wedge y) \llcorner u^* = (x \llcorner u^*) \wedge y + (-1)^r x \wedge (y \llcorner u^*),$$

for every $u^* \in E$, $\in \bigwedge^r E$, and $y \in \bigwedge^{q+1-r} E$. This formula is used by Shafarevitch [156] to define a hook, but beware that Shafarevitch use the left hook notation $u^* \lrcorner x$ rather than the right hook notation. Shafarevitch uses the terminology *convolution*, which seems very unfortunate.

For $u \in E$, the right hook $z^* \llcorner u$ is also denoted $i(u)z^*$, and called *insertion operator* or *interior product*. This operator plays an important role in differential geometry.

Definition 34.12. Let $u \in E$ and $z^* \in \bigwedge^{n+1}(E^*)$. If we view z^* as an alternating multilinear map in $\mathrm{Alt}^{n+1}(E; K)$, then we define $i(u)z^* \in \mathrm{Alt}^n(E; K)$ as given by

$$(i(u)z^*)(v_1, \ldots, v_n) = z^*(u, v_1, \ldots, v_n).$$

Using the left hook $\lrcorner$ and the right hook $\llcorner$ we can define two linear maps $\gamma\colon \bigwedge^p E \to \bigwedge^{n-p} E^*$ and $\delta\colon \bigwedge^p E^* \to \bigwedge^{n-p} E$ as follows:

Definition 34.13. For any basis $(e_1, \ldots, e_n)$ of E, if we let $M = \{1, \ldots, n\}$, $e = e_1 \wedge \cdots \wedge e_n$, and $e^* = e_1^* \wedge \cdots \wedge e_n^*$, define $\gamma\colon \bigwedge^p E \to \bigwedge^{n-p} E^*$ and $\delta\colon \bigwedge^p E^* \to \bigwedge^{n-p} E$ as

$$\gamma(u) = u \lrcorner e^* \quad \text{and} \quad \delta(v^*) = e \llcorner v^*,$$

for all $u \in \bigwedge^p E$ and all $v^* \in \bigwedge^p E^*$.

Proposition 34.23. *The linear maps $\gamma\colon \bigwedge^p E \to \bigwedge^{n-p} E^*$ and $\delta\colon \bigwedge^p E^* \to \bigwedge^{n-p} E$ are isomorphims, and $\gamma^{-1} = \delta$. The isomorphisms γ and δ map decomposable vectors to decomposable vectors. Furthermore, if $z \in \bigwedge^p E$ is decomposable, say $z = u_1 \wedge \cdots \wedge u_p$ for some $u_i \in E$, then $\gamma(z) = v_1^* \wedge \cdots \wedge v_{n-p}^*$ for some $v_j^* \in E^*$, and $v_j^*(u_i) = 0$ for all i, j. A similar property holds for $v^* \in \bigwedge^p E^*$ and $\delta(v^*)$. If $(e_1', \ldots, e_n')$ is any other basis of E and $\gamma'\colon \bigwedge^p E \to \bigwedge^{n-p} E^*$ and $\delta'\colon \bigwedge^p E^* \to \bigwedge^{n-p} E$ are the corresponding isomorphisms, then $\gamma' = \lambda\gamma$ and $\delta' = \lambda^{-1}\delta$ for some nonzero $\lambda \in K$.*

Proof. Using Propositions 34.18 and 34.21, for any subset $J \subseteq \{1, \ldots, n\} = M$ such that $|J| = p$, we have

$$\gamma(e_J) = e_J \lrcorner e^* = \rho_{M-J,J} e_{M-J}^* \quad \text{and} \quad \delta(e_{M-J}^*) = e \llcorner e_{M-J}^* = \rho_{M-J,J} e_J.$$

Thus,

$$\delta \circ \gamma(e_J) = \rho_{M-J,J}\rho_{M-J,J} e_J = e_J,$$

since $\rho_{M-J,J} = \pm 1$. A similar result holds for $\gamma \circ \delta$. This implies that

$$\delta \circ \gamma = \mathrm{id} \quad \text{and} \quad \gamma \circ \delta = \mathrm{id}.$$

Thus, γ and δ are inverse isomorphisms.

If $z \in \bigwedge^p E$ is decomposable, then $z = u_1 \wedge \cdots \wedge u_p$ where $u_1, \ldots, u_p$ are linearly independent since $z \neq 0$, and we can pick a basis of E of the form $(u_1, \ldots, u_n)$. Then the above formulae show that

$$\gamma(z) = \pm u_{p+1}^* \wedge \cdots \wedge u_n^*.$$

Since $(u_1^*, \ldots, u_n^*)$ is the dual basis of $(u_1, \ldots, u_n)$, we have $u_i^*(u_j) = \delta_{ij}$, If $(e_1', \ldots, e_n')$ is any other basis of E, because $\bigwedge^n E$ has dimension 1, we have

$$e_1' \wedge \cdots \wedge e_n' = \lambda e_1 \wedge \cdots \wedge e_n$$

for some nonzero $\lambda \in K$, and the rest is trivial. □

Applying Proposition 34.23 to the case where $p = n - 1$, the isomorphism $\gamma\colon \bigwedge^{n-1} E \to \bigwedge^1 E^*$ maps indecomposable vectors in $\bigwedge^{n-1} E$ to indecomposable vectors in $\bigwedge^1 E^* = E^*$. But every vector in E^* is decomposable, so every vector in $\bigwedge^{n-1} E$ is decomposable.

Corollary 34.24. *If E is a finite-dimensional vector space, then every vector in $\bigwedge^{n-1} E$ is decomposable.*

34.8 Testing Decomposability ⊛

We are now ready to tackle the problem of finding criteria for decomposability. Such criteria will use the left hook. Once again, in this section *all vector spaces are assumed to have finite dimension*. But before stating our criteria, we need a few preliminary results.

Proposition 34.25. *Given $z \in \bigwedge^p E$ with $z \neq 0$, the smallest vector space $W \subseteq E$ such that $z \in \bigwedge^p W$ is generated by the vectors of the form*

$$u^* \lrcorner z, \qquad \text{with } u^* \in {\textstyle\bigwedge^{p-1}} E^*.$$

Proof. First let W be any subspace such that $z \in \bigwedge^p(W)$ and let $(e_1, \ldots, e_r, e_{r+1}, \ldots, e_n)$ be a basis of E such that $(e_1, \ldots, e_r)$ is a basis of W. Then, $u^* = \sum_I \lambda_I e_I^*$, where $I \subseteq \{1, \ldots, n\}$ and $|I| = p - 1$, and $z = \sum_J \mu_J e_J$, where $J \subseteq \{1, \ldots, r\}$ and $|J| = p \leq r$. It follows immediately from the formula of Proposition 34.18 (4), namely

$$e_I^* \lrcorner e_J = \rho_{J-I,J} e_{J-I},$$

that $u^* \lrcorner z \in W$, since $J - I \subseteq \{1, \ldots, r\}$.

Next we prove that if W is the smallest subspace of E such that $z \in \bigwedge^p(W)$, then W is generated by the vectors of the form $u^* \lrcorner z$, where $u^* \in \bigwedge^{p-1} E^*$. Suppose not. Then the vectors $u^* \lrcorner z$ with $u^* \in \bigwedge^{p-1} E^*$ span a proper subspace U of W. We prove that for every subspace W' of W with $\dim(W') = \dim(W) - 1 = r - 1$, it is not possible that $u^* \lrcorner z \in W'$ for all $u^* \in \bigwedge^{p-1} E^*$. But then, as U is a proper subspace of W, it is contained in some subspace W' with $\dim(W') = r - 1$, and we have a contradiction.

Let $w \in W - W'$ and pick a basis of W formed by a basis $(e_1, \ldots, e_{r-1})$ of W' and w. Any $z \in \bigwedge^p(W)$ can be written as $z = z' + w \wedge z''$, where $z' \in \bigwedge^p W'$ and $z'' \in \bigwedge^{p-1} W'$, and since W is the smallest subspace containing z, we have $z'' \neq 0$. Consequently, if we write $z'' = \sum_I \lambda_I e_I$ in terms of the basis $(e_1, \ldots, e_{r-1})$ of W', there is some e_I, with $I \subseteq \{1, \ldots, r-1\}$ and $|I| = p - 1$, so that the coefficient λ_I is nonzero. Now, using any basis of E containing $(e_1, \ldots, e_{r-1}, w)$, by Proposition 34.18 (4), we see that

$$e_I^* \lrcorner (w \wedge e_I) = \lambda w, \qquad \lambda = \pm 1.$$

It follows that

$$e_I^* \lrcorner z = e_I^* \lrcorner (z' + w \wedge z'') = e_I^* \lrcorner z' + e_I^* \lrcorner (w \wedge z'') = e_I^* \lrcorner z' + \lambda \lambda_I w,$$

with $e_I^* \lrcorner z' \in W'$, which shows that $e_I^* \lrcorner z \notin W'$. Therefore, W is indeed generated by the vectors of the form $u^* \lrcorner z$, where $u^* \in \bigwedge^{p-1} E^*$. □

To help understand Proposition 34.25, let E be the vector space with basis $\{e_1, e_2, e_3, e_4\}$ and $z = e_1 \wedge e_2 + e_2 \wedge e_3$. Note that $z \in \bigwedge^2 E$. To find the smallest vector space $W \subseteq E$

such that $z \in \bigwedge^2 W$, we calculate $u^* \lrcorner z$, where $u^* \in \bigwedge^1 E^*$. The multilinearity of $\lrcorner$ implies it is enough to calculate $u^* \lrcorner z$ for $u^* \in \{e_1^*, e_2^*, e_3^*, e_4^*\}$. Proposition 34.18 (4) implies that

$$\begin{aligned}
e_1^* \lrcorner z &= e_1^* \lrcorner (e_1 \wedge e_2 + e_2 \wedge e_3) = e_1^* \lrcorner e_1 \wedge e_2 = -e_2\\
e_2^* \lrcorner z &= e_2^* \lrcorner (e_1 \wedge e_2 + e_2 \wedge e_3) = e_1 - e_3\\
e_3^* \lrcorner z &= e_3^* \lrcorner (e_1 \wedge e_2 + e_2 \wedge e_3) = e_3^* \lrcorner e_2 \wedge e_3 = e_2\\
e_4^* \lrcorner z &= e_4^* \lrcorner (e_1 \wedge e_2 + e_2 \wedge e_3) = 0.
\end{aligned}$$

Thus W is the two-dimensional vector space generated by the basis $\{e_2, e_1 - e_3\}$. This is not surprising since $z = -e_2 \wedge (e_1 - e_3)$ and is in fact decomposable. As this example demonstrates, the action of the left hook provides a way of extracting a basis of W from z.

Proposition 34.25 implies the following corollary.

Corollary 34.26. *Any nonzero $z \in \bigwedge^p E$ is decomposable iff the smallest subspace W of E such that $z \in \bigwedge^p W$ has dimension p. Furthermore, if $z = u_1 \wedge \cdots \wedge u_p$ is decomposable, then $(u_1, \ldots, u_p)$ is a basis of the smallest subspace W of E such that $z \in \bigwedge^p W$*

Proof. If $\dim(W) = p$, then for any basis $(e_1, \ldots, e_p)$ of W we know that $\bigwedge^p W$ has $e_1 \wedge \cdots \wedge e_p$ has a basis, and thus has dimension 1. Since $z \in \bigwedge^p W$, we have $z = \lambda e_1 \wedge \cdots \wedge e_p$ for some nonzero λ, so z is decomposable.

Conversely assume that $z \in \bigwedge^p W$ is nonzero and decomposable. Then, $z = u_1 \wedge \cdots \wedge u_p$, and since $z \neq 0$, by Proposition 34.8 $(u_1, \ldots, u_p)$ are linearly independent. Then for any $v_i^* = u_1^* \wedge \cdots u_{i-1}^* \wedge u_{i+1}^* \wedge \cdots \wedge u_p^*$ (where u_i^* is omitted), we have

$$v_i^* \lrcorner z = (u_1^* \wedge \cdots u_{i-1}^* \wedge u_{i+1}^* \wedge \cdots \wedge u_p^*) \lrcorner (u_1 \wedge \cdots \wedge u_p) = \pm u_i,$$

so by Proposition 34.25 we have $u_i \in W$ for $i = 1, \ldots, p$. This shows that $\dim(W) \geq p$, but since $z = u_1 \wedge \cdots \wedge u_p$, we have $\dim(W) = p$, which means that $(u_1, \ldots, u_p)$ is a basis of W. □

Finally we are ready to state and prove the criterion for decomposability with respect to left hooks.

Proposition 34.27. *Any nonzero $z \in \bigwedge^p E$ is decomposable iff*

$$(u^* \lrcorner z) \wedge z = 0, \qquad \textit{for all } u^* \in \textstyle\bigwedge^{p-1} E^*.$$

Proof. First assume that $z \in \bigwedge^p E$ is decomposable. If so, by Corollary 34.26, the smallest subspace W of E such that $z \in \bigwedge^p W$ has dimension p, so we have $z = e_1 \wedge \cdots \wedge e_p$ where $e_1, \ldots, e_p$ form a basis of W. By Proposition 34.25, for every $u^* \in \bigwedge^{p-1} E^*$, we have $u^* \lrcorner z \in W$, so each $u^* \lrcorner z$ is a linear combination of the e_i's, say

$$u^* \lrcorner z = \alpha_1 e_1 + \cdots + \alpha_p e_p,$$

and

$$(u^* \lrcorner z) \wedge z = \sum_{i=1}^{p} \alpha_i e_i \wedge e_1 \wedge \cdots \wedge e_i \wedge \cdots \wedge e_p = 0.$$

Now assume that $(u^* \lrcorner z) \wedge z = 0$ for all $u^* \in \bigwedge^{p-1} E^*$, and that $\dim(W) = m > p$, where W is the smallest subspace of E such that $z \in \bigwedge^p W$ If $e_1, \ldots, e_m$ is a basis of W, then we have $z = \sum_I \lambda_I e_I$, where $I \subseteq \{1, \ldots, m\}$ and $|I| = p$. Recall that $z \neq 0$, and so, some λ_I is nonzero. By Proposition 34.25, each e_i can be written as $u^* \lrcorner z$ for some $u^* \in \bigwedge^{p-1} E^*$, and since $(u^* \lrcorner z) \wedge z = 0$ for all $u^* \in \bigwedge^{p-1} E^*$, we get

$$e_j \wedge z = 0 \quad \text{for} \quad j = 1, \ldots, m.$$

By wedging $z = \sum_I \lambda_I e_I$ with each e_j, as $m > p$, we deduce $\lambda_I = 0$ for all I, so $z = 0$, a contradiction. Therefore, $m = p$ and Corollary 34.26 implies that z is decomposable. □

As a corollary of Proposition 34.27 we obtain the following fact that we stated earlier without proof.

Proposition 34.28. *Given any vector space E of dimension n, a vector $x \in \bigwedge^2 E$ is decomposable iff $x \wedge x = 0$.*

Proof. Recall that as an application of Proposition 34.19 we proved the formula (†), namely

$$u^* \lrcorner (x \wedge x) = 2((u^* \lrcorner x) \wedge x)$$

for all $x \in \bigwedge^2 E$ and all $u^* \in E^*$. As a consequence, $(u^* \lrcorner x) \wedge x = 0$ iff $u^* \lrcorner (x \wedge x) = 0$. By Proposition 34.27, the 2-vector x is decomposable iff $u^* \lrcorner (x \wedge x) = 0$ for all $u^* \in E^*$ iff $x \wedge x = 0$. Therefore, a 2-vector x is decomposable iff $x \wedge x = 0$. □

As an application of Proposition 34.28, assume that $\dim(E) = 3$ and that (e_1, e_2, e_3) is a basis of E. Then any 2-vector $x \in \bigwedge^2 E$ is of the form

$$x = \alpha e_1 \wedge e_2 + \beta e_1 \wedge e_3 + \gamma e_2 \wedge e_3.$$

We have

$$x \wedge x = (\alpha e_1 \wedge e_2 + \beta e_1 \wedge e_3 + \gamma e_2 \wedge e_3) \wedge (\alpha e_1 \wedge e_2 + \beta e_1 \wedge e_3 + \gamma e_2 \wedge e_3) = 0,$$

because all the terms involved are of the form $c\, e_{i_1} \wedge e_{i_2} \wedge e_{i_3} \wedge e_{i_4}$ with $i_1, i_2, i_3, i_4 \in \{1, 2, 3\}$, and so at least two of these indices are identical. Therefore, every 2-vector $x = \alpha e_1 \wedge e_2 + \beta e_1 \wedge e_3 + \gamma e_2 \wedge e_3$ is decomposable, although this not obvious at first glance. For example,

$$e_1 \wedge e_2 + e_1 \wedge e_3 + e_2 \wedge e_3 = (e_1 + e_2) \wedge (e_2 + e_3).$$

We now show that Proposition 34.27 yields an equational criterion for the decomposability of an alternating tensor $z \in \bigwedge^p E$.

34.9 The Grassmann-Plücker's Equations and Grassmannian Manifolds ⊛

We follow an argument adapted from Bourbaki [25] (Chapter III, §11, Section 13).

Let E be a vector space of dimensions n, let $(e_1, \ldots, e_n)$ be a basis of E, and let $(e_1^*, \ldots, e_n^*)$ be its dual basis. Our objective is to determine whether a nonzero vector $z \in \bigwedge^p E$ is decomposable. By Proposition 34.27, the vector z is decomposable iff $(u^* \lrcorner z) \wedge z = 0$ for all $u^* \in \bigwedge^{p-1} E^*$. We can let u^* range over a basis of $\bigwedge^{p-1} E^*$, and then the conditions are

$$(e_H^* \lrcorner z) \wedge z = 0$$

for all $H \subseteq \{1, \ldots, n\}$, with $|H| = p - 1$. Since $(e_H^* \lrcorner z) \wedge z \in \bigwedge^{p+1} E$, this is equivalent to

$$\langle e_J^*, (e_H^* \lrcorner z) \wedge z \rangle = 0$$

for all $H, J \subseteq \{1, \ldots, n\}$, with $|H| = p - 1$ and $|J| = p + 1$. Then, for all $I, I' \subseteq \{1, \ldots, n\}$ with $|I| = |I'| = p$, Formulae (2) and (4) of Proposition 34.18 show that

$$\langle e_J^*, (e_H^* \lrcorner e_I) \wedge e_{I'} \rangle = 0,$$

unless there is some $i \in \{1, \ldots, n\}$ such that

$$I - H = \{i\}, \quad J - I' = \{i\}.$$

In this case, $I = H \cup \{i\}$ and $I' = J - \{i\}$, and using Formulae (2) and (4) of Proposition 34.18, we have

$$\langle e_J^*, (e_H^* \lrcorner e_{H \cup \{i\}}) \wedge e_{J-\{i\}} \rangle = \langle e_J^*, \rho_{\{i\},H} e_i \wedge e_{J-\{i\}} \rangle = \langle e_J^*, \rho_{\{i\},H} \rho_{\{i\},J-\{i\}} e_J \rangle = \rho_{\{i\},H} \rho_{\{i\},J-\{i\}}.$$

If we let

$$\epsilon_{i,J,H} = \rho_{\{i\},H} \rho_{\{i\},J-\{i\}},$$

we have $\epsilon_{i,J,H} = +1$ if the parity of the number of $j \in J$ such that $j < i$ is the same as the parity of the number of $h \in H$ such that $h < i$, and $\epsilon_{i,J,H} = -1$ otherwise.

Finally we obtain the following criterion in terms of quadratic equations (*Plücker's equations*) for the decomposability of an alternating tensor.

Proposition 34.29. *(Grassmann-Plücker's Equations) For $z = \sum_I \lambda_I e_I \in \bigwedge^p E$, the conditions for $z \neq 0$ to be decomposable are*

$$\sum_{i \in J - H} \epsilon_{i,J,H} \lambda_{H \cup \{i\}} \lambda_{J - \{i\}} = 0,$$

with $\epsilon_{i,J,H} = \rho_{\{i\},H} \rho_{\{i\},J-\{i\}}$, for all $H, J \subseteq \{1, \ldots, n\}$ such that $|H| = p - 1$, $|J| = p + 1$, and all $i \in J - H$.

Using the above criterion, it is a good exercise to reprove that if $\dim(E) = n$, then every tensor in $\bigwedge^{n-1}(E)$ is decomposable. We already proved this fact as a corollary of Proposition 34.23.

Given any $z = \sum_I \lambda_I e_I \in \bigwedge^p E$ where $\dim(E) = n$, the family of scalars (λ_I) (with $I = \{i_1 < \cdots < i_p\} \subseteq \{1, \ldots, n\}$ listed in increasing order) is called the *Plücker coordinates* of z.The Grassmann-Plücker's equations give necessary and sufficient conditions for any nonzero z to be decomposable.

For example, when $\dim(E) = n = 4$ and $p = 2$, these equations reduce to the single equation

$$\lambda_{12}\lambda_{34} - \lambda_{13}\lambda_{24} + \lambda_{14}\lambda_{23} = 0.$$

However, it should be noted that the equations given by Proposition 34.29 are not independent in general.

We are now in the position to prove that the Grassmannian $G(p, n)$ can be embedded in the projective space $\mathbb{RP}^{\binom{n}{p}-1}$,

For any $n \geq 1$ and any k with $1 \leq p \leq n$, recall that the Grassmannian $G(p, n)$ is the set of all linear p-dimensional subspaces of $\mathbb{R}^n$ (also called *p-planes*). Any p-dimensional subspace U of $\mathbb{R}^n$ is spanned by p linearly independent vectors $u_1, \ldots, u_p$ in $\mathbb{R}^n$; write $U = \mathrm{span}(u_1, \ldots, u_k)$. By Proposition 34.8, $(u_1, \ldots, u_p)$ are linearly independent iff $u_1 \wedge \cdots \wedge u_p \neq 0$. If $(v_1, \ldots, v_p)$ are any other linearly independent vectors spanning U, then we have

$$v_j = \sum_{i=1}^{p} a_{ij} u_i, \quad 1 \leq j \leq p,$$

for some $a_{ij} \in \mathbb{R}$, and by Proposition 34.2

$$v_1 \wedge \cdots \wedge v_p = \det(A)\, u_1 \wedge \cdots \wedge u_p,$$

where $A = (a_{ij})$. As a consequence, we can define a map $i_G \colon G(p, n) \to \mathbb{RP}^{\binom{n}{p}-1}$ such that for any k-plane U, for any basis $(u_1, \ldots, u_p)$ of U,

$$i_G(U) = [u_1 \wedge \cdots \wedge u_p],$$

the point of $\mathbb{RP}^{\binom{n}{p}-1}$ given by the one-dimensional subspace of $\mathbb{R}^{\binom{n}{p}}$ spanned by $u_1 \wedge \cdots \wedge u_p$.

Proposition 34.30. *The map $i_G \colon G(p, n) \to \mathbb{RP}^{\binom{n}{p}-1}$ is injective.*

Proof. Let U and V be any two p-planes and assume that $i_G(U) = i_G(V)$. This means that there is a basis $(u_1, \ldots, u_p)$ of U and a basis $(v_1, \ldots, v_p)$ of V such that

$$v_1 \wedge \cdots \wedge v_p = c\, u_1 \wedge \cdots \wedge u_p$$

for some nonzero $c \in \mathbb{R}$. The above implies that the smallest subspaces W and W' of $\mathbb{R}^n$ such that $u_1 \wedge \cdots \wedge u_p \in \bigwedge^p W$ and $v_1 \wedge \cdots \wedge v_p \in \bigwedge^p W'$ are identical, so $W = W'$. By Corollary 34.26, this smallest subspace W has both $(u_1, \ldots, u_p)$ and $(v_1, \ldots, v_p)$ as bases, so the v_j are linear combinations of the u_i (and vice-versa), and $U = V$. □

Since any nonzero $z \in \bigwedge^p \mathbb{R}^n$ can be uniquely written as

$$z = \sum_I \lambda_I e_I$$

in terms of its Plücker coordinates (λ_I), every point of $\mathbb{RP}^{\binom{n}{p}-1}$ is defined by the Plücker coordinates (λ_I) viewed as homogeneous coordinates. The points of $\mathbb{RP}^{\binom{n}{p}-1}$ corresponding to one-dimensional spaces associated with decomposable alternating p-tensors are the points whose coordinates satisfy the Grassmann-Plücker's equations of Proposition 34.29. Therefore, the map i_G embeds the Grassmannian $G(p, n)$ as an algebraic variety in $\mathbb{RP}^{\binom{n}{p}-1}$ defined by equations of degree 2.

We can replace the field $\mathbb{R}$ by $\mathbb{C}$ in the above reasoning and we obtain an embedding of the complex Grassmannian $G_{\mathbb{C}}(p, n)$ as an algebraic variety in $\mathbb{CP}^{\binom{n}{p}-1}$ defined by equations of degree 2.

In particular, if $n = 4$ and $p = 2$, the equation

$$\lambda_{12}\lambda_{34} - \lambda_{13}\lambda_{24} + \lambda_{14}\lambda_{23} = 0$$

is the homogeneous equation of a quadric in $\mathbb{CP}^5$ known as the *Klein quadric*. The points on this quadric are in one-to-one correspondence with the lines in $\mathbb{CP}^3$.

There is also a simple algebraic criterion to decide whether the smallest subspaces U and V associated with two nonzero decomposable vectors $u_1 \wedge \cdots \wedge u_p$ and $v_1 \wedge \cdots \wedge v_q$ have a nontrivial intersection.

Proposition 34.31. *Let E be any n-dimensional vector space over a field K, and let U and V be the smallest subspaces of E associated with two nonzero decomposable vectors $u = u_1 \wedge \cdots \wedge u_p \in \bigwedge^p U$ and $v = v_1 \wedge \cdots \wedge v_q \in \bigwedge^q V$. The following properties hold:*

(1) We have $U \cap V = (0)$ iff $u \wedge v \neq 0$.

(2) If $U \cap V = (0)$, then $U + V$ is the least subspace associated with $u \wedge v$.

Proof. Assume $U \cap V = (0)$. We know by Corollary 34.26 that $(u_1, \ldots, u_p)$ is a basis of U and $(v_1, \ldots, v_q)$ is a basis of V. Since $U \cap V = (0)$, $(u_1, \ldots, u_p, v_1, \ldots, v_q)$ is a basis of $U + V$, and by Proposition 34.8, we have

$$u \wedge v = u_1 \wedge \cdots \wedge u_p \wedge v_1 \wedge \cdots \wedge v_q \neq 0.$$

This also proves (2).

Conversely, assume that $\dim(U \cap V) \geq 1$. Pick a basis $(w_1, \ldots, w_r)$ of $W = U \cap V$, and extend this basis to a basis $(w_1, \ldots, w_r, w_{r+1}, \ldots, w_p)$ of U and to a basis $(w_1, \ldots, w_r, w_{p+1}, \ldots, w_{p+q-r})$ of V. By Corollary 34.26, $(u_1, \ldots, u_p)$ is also basis of U, so

$$u_1 \wedge \cdots \wedge u_p = a\, w_1 \wedge \cdots \wedge w_r \wedge w_{r+1} \wedge \cdots \wedge w_p$$

for some $a \in K$, and $(v_1, \ldots, v_q)$ is also basis of V, so

$$v_1 \wedge \cdots \wedge v_q = b\, w_1 \cdots \wedge w_r \wedge w_{p+1} \wedge \cdots \wedge w_{p+q-r}$$

for some $b \in K$, and thus

$$u \wedge v = u_1 \wedge \cdots \wedge u_p \wedge v_1 \wedge \cdots \wedge v_q = 0$$

since it contains some repeated w_i, with $1 \leq i \leq r$. □

As an application of Proposition 34.31, consider two projective lines D_1 and D_2 in $\mathbb{RP}^3$, which means that D_1 and D_2 correspond to two 2-planes in $\mathbb{R}^4$, and thus by Proposition 34.30, to two points in $\mathbb{RP}^{\binom{4}{2}-1} = \mathbb{RP}^5$. These two points correspond to the 2-vectors

$$z = a_{1,2}e_1 \wedge e_2 + a_{1,3}e_1 \wedge e_3 + a_{1,4}e_1 \wedge e_4 + a_{2,3}e_2 \wedge e_3 + a_{2,4}e_2 \wedge e_4 + a_{3,4}e_3 \wedge e_4$$

and

$$z' = a'_{1,2}e_1 \wedge e_2 + a'_{1,3}e_1 \wedge e_3 + a'_{1,4}e_1 \wedge e_4 + a'_{2,3}e_2 \wedge e_3 + a'_{2,4}e_2 \wedge e_4 + a'_{3,4}e_3 \wedge e_4$$

whose Plücker coordinates, (where $a_{i,j} = \lambda_{ij}$), satisfy the equation

$$\lambda_{12}\lambda_{34} - \lambda_{13}\lambda_{24} + \lambda_{14}\lambda_{23} = 0$$

of the Klein quadric, and D_1 and D_2 intersect iff $z \wedge z' = 0$ iff

$$a_{1,2}a'_{3,4} - a_{1,3}a'_{3,4} + a_{1,4}a'_{2,3} + a_{2,3}a'_{1,4} - a_{2,4}a'_{1,3} + a_{3,4}a'_{1,2} = 0.$$

Observe that for D_1 fixed, this is a linear condition. This fact is very helpful for solving problems involving intersections of lines. A famous problem is to find how many lines in $\mathbb{RP}^3$ meet four given lines in general position. The answer is at most 2.

34.10 Vector-Valued Alternating Forms

The purpose of this section is to present the technical background needed to understand vector-valued differential forms, in particular in the case of Lie groups where differential forms taking their values in a Lie algebra arise naturally.

In this section the vector space E is assumed to have *finite dimension*. We know that there is a canonical isomorphism $\bigwedge^n(E^*) \cong \mathrm{Alt}^n(E; K)$ between alternating n-forms and alternating multilinear maps. As in the case of general tensors, the isomorphisms provided by Propositions 34.5, 33.17, and 34.10, namely

$$\begin{aligned}\mathrm{Alt}^n(E;F) &\cong \mathrm{Hom}\Big(\bigwedge^n(E),F\Big)\\ \mathrm{Hom}\Big(\bigwedge^n(E),F\Big) &\cong \Big(\bigwedge^n(E)\Big)^*\otimes F\\ \Big(\bigwedge^n(E)\Big)^* &\cong \bigwedge^n(E^*)\end{aligned}$$

yield a canonical isomorphism

$$\mathrm{Alt}^n(E;F)\cong\Big(\bigwedge^n(E^*)\Big)\otimes F$$

which we record as a corollary.

Corollary 34.32. *For any finite-dimensional vecgtor space E and any vector space F, we have a canonical isomorphism*

$$\mathrm{Alt}^n(E;F)\cong\Big(\bigwedge^n(E^*)\Big)\otimes F.$$

Note that F may have infinite dimension. This isomorphism allows us to view the tensors in $\bigwedge^n(E^*)\otimes F$ as *vector-valued alternating forms*, a point of view that is useful in differential geometry. If $(f_1,\ldots,f_r)$ is a basis of F, every tensor $\omega\in\bigwedge^n(E^*)\otimes F$ can be written as some linear combination

$$\omega=\sum_{i=1}^r\alpha_i\otimes f_i,$$

with $\alpha_i\in\bigwedge^n(E^*)$.We also let

$$\bigwedge(E;F)=\bigoplus_{n=0}\Big(\bigwedge^n(E^*)\Big)\otimes F=\Big(\bigwedge(E)\Big)\otimes F.$$

Given three vector spaces, F,G,H, if we have some bilinear map $\Phi\colon F\times G\to H$, then we can define a multiplication operation

$$\wedge_\Phi\colon\bigwedge(E;F)\times\bigwedge(E;G)\to\bigwedge(E;H)$$

as follows: For every pair (m,n), we define the multiplication

$$\wedge_\Phi\colon\bigg(\Big(\bigwedge^m(E^*)\Big)\otimes F\bigg)\times\bigg(\Big(\bigwedge^n(E^*)\Big)\otimes G\bigg)\longrightarrow\Big(\bigwedge^{m+n}(E^*)\Big)\otimes H$$

by

$$\omega \wedge_\Phi \eta = (\alpha \otimes f) \wedge_\Phi (\beta \otimes g) = (\alpha \wedge \beta) \otimes \Phi(f, g).$$

As in Section 34.5 (following H. Cartan [35]), we can also define a multiplication

$$\wedge_\Phi \colon \mathrm{Alt}^m(E; F) \times \mathrm{Alt}^n(E; G) \longrightarrow \mathrm{Alt}^{m+n}(E; H)$$

directly on alternating multilinear maps as follows: For $f \in \mathrm{Alt}^m(E; F)$ and $g \in \mathrm{Alt}^n(E; G)$,

$$(f \wedge_\Phi g)(u_1, \ldots, u_{m+n}) = \sum_{\sigma \in \mathrm{shuffle}(m,n)} \mathrm{sgn}(\sigma)\, \Phi\Big(f(u_{\sigma(1)}, \ldots, u_{\sigma(m)}), g(u_{\sigma(m+1)}, \ldots, u_{\sigma(m+n)})\Big),$$

where shuffle(m, n) consists of all (m, n)-"shuffles;" that is, permutations σ of $\{1, \ldots m + n\}$ such that $\sigma(1) < \cdots < \sigma(m)$ and $\sigma(m + 1) < \cdots < \sigma(m + n)$.

A special case of interest is the case where $F = G = H$ is a Lie algebra and $\Phi(a, b) = [a, b]$ is the Lie bracket of F. In this case, using a basis $(f_1, \ldots, f_r)$ of F, if we write $\omega = \sum_i \alpha_i \otimes f_i$ and $\eta = \sum_j \beta_j \otimes f_j$, we have

$$\omega \wedge_\Phi \eta = [\omega, \eta] = \sum_{i,j} \alpha_i \wedge \beta_j \otimes [f_i, f_j].$$

It is customary to denote $\omega \wedge_\Phi \eta$ by $[\omega, \eta]$ (unfortunately, the bracket notation is overloaded). Consequently,

$$[\eta, \omega] = (-1)^{mn+1}[\omega, \eta].$$

In general not much can be said about $\wedge_\Phi$, unless Φ has some additional properties. In particular, $\wedge_\Phi$ is generally not associative.

We now use vector-valued alternating forms to generalize both the μ map of Proposition 34.14 and generalize Proposition 33.17 by defining the map

$$\mu_F \colon \left(\bigwedge^n (E^*)\right) \otimes F \longrightarrow \mathrm{Alt}^n(E; F)$$

on generators by

$$\mu_F((v_1^* \wedge \cdots \wedge v_n^*) \otimes f)(u_1, \ldots, u_n) = (\det(v_j^*(u_i))f,$$

with $v_1^*, \ldots, v_n^* \in E^*$, $u_1, \ldots, u_n \in E$, and $f \in F$.

Proposition 34.33. *The map*

$$\mu_F \colon \left(\bigwedge^n (E^*)\right) \otimes F \longrightarrow \mathrm{Alt}^n(E; F)$$

defined as above is a canonical isomorphism for every $n \geq 0$. Furthermore, given any three vector spaces, F, G, H, and any bilinear map $\Phi \colon F \times G \to H$, for all $\omega \in (\bigwedge^n (E^*)) \otimes F$ and all $\eta \in (\bigwedge^n (E^*)) \otimes G$,

$$\mu_H(\omega \wedge_\Phi \eta) = \mu_F(\omega) \wedge_\Phi \mu_G(\eta).$$

Proof. Since we already know that $(\bigwedge^n(E^*))\otimes F$ and $\mathrm{Alt}^n(E;F)$ are isomorphic, it is enough to show that μ_F maps some basis of $(\bigwedge^n(E^*))\otimes F$ to linearly independent elements. Pick some bases $(e_1,\ldots,e_p)$ in E and $(f_j)_{j\in J}$ in F. Then we know that the vectors $e_I^*\otimes f_j$, where $I\subseteq\{1,\ldots,p\}$ and $|I|=n$, form a basis of $(\bigwedge^n(E^*))\otimes F$. If we have a linear dependence

$$\sum_{I,j}\lambda_{I,j}\mu_F(e_I^*\otimes f_j)=0,$$

applying the above combination to each $(e_{i_1},\ldots,e_{i_n})$ ($I=\{i_1,\ldots,i_n\}$, $i_1<\cdots<i_n$), we get the linear combination

$$\sum_j\lambda_{I,j}f_j=0,$$

and by linear independence of the f_j's, we get $\lambda_{I,j}=0$ for all I and all j. Therefore, the $\mu_F(e_I^*\otimes f_j)$ are linearly independent, and we are done. The second part of the proposition is checked using a simple computation. □

The following proposition will be useful in dealing with vector-valued differential forms.

Proposition 34.34. *If $(e_1,\ldots,e_p)$ is any basis of E, then every element $\omega\in(\bigwedge^n(E^*))\otimes F$ can be written in a unique way as*

$$\omega=\sum_I e_I^*\otimes f_I,\qquad f_I\in F,$$

where the e_I^* are defined as in Section 34.2.

Proof. Since, by Proposition 34.7, the e_I^* form a basis of $\bigwedge^n(E^*)$, elements of the form $e_I^*\otimes f$ span $(\bigwedge^n(E^*))\otimes F$. Now if we apply $\mu_F(\omega)$ to $(e_{i_1},\ldots,e_{i_n})$, where $I=\{i_1,\ldots,i_n\}\subseteq\{1,\ldots,p\}$, we get

$$\mu_F(\omega)(e_{i_1},\ldots,e_{i_n})=\mu_F(e_I^*\otimes f_I)(e_{i_1},\ldots,e_{i_n})=f_I.$$

Therefore, the f_I are uniquely determined by f. □

Proposition 34.34 can also be formulated in terms of alternating multilinear maps, a fact that will be useful to deal with differential forms.

Corollary 34.35. *Define the product $\cdot\colon\mathrm{Alt}^n(E;\mathbb{R})\times F\to\mathrm{Alt}^n(E;F)$ as follows: For all $\omega\in\mathrm{Alt}^n(E;\mathbb{R})$ and all $f\in F$,*

$$(\omega\cdot f)(u_1,\ldots,u_n)=\omega(u_1,\ldots,u_n)f,$$

for all $u_1,\ldots,u_n\in E$. Then for every $\omega\in(\bigwedge^n(E^*))\otimes F$ of the form

$$\omega=u_1^*\wedge\cdots\wedge u_n^*\otimes f,$$

we have

$$\mu_F(u_1^*\wedge\cdots\wedge u_n^*\otimes f)=\mu_F(u_1^*\wedge\cdots\wedge u_n^*)\cdot f.$$

Then Proposition 34.34 yields the following result.

Proposition 34.36. *If $(e_1, \ldots, e_p)$ is any basis of E, then every element $\omega \in \mathrm{Alt}^n(E; F)$ can be written in a unique way as*

$$\omega = \sum_I e_I^* \cdot f_I, \qquad f_I \in F,$$

where the e_I^* are defined as in Section 34.2.

34.11 Problems

Problem 34.1. Complete the induction argument used in the proof of Proposition 34.1 (2).

Problem 34.2. Prove Proposition 34.2.

Problem 34.3. Prove Proposition 34.9.

Problem 34.4. Show that the pairing given by $(*)$ in Section 34.4 is nondegenerate.

Problem 34.5. Let $\mathfrak{I}_a$ be the two-sided ideal generated by all tensors of the form $u \otimes u \in V^{\otimes 2}$. Prove that

$$\bigwedge^m(V) \cong V^{\otimes m}/(\mathfrak{I}_a \cap V^{\otimes m}).$$

Problem 34.6. Complete the induction proof of Proposition 34.12.

Problem 34.7. Prove the following lemma: If V is a vector space with $\dim(V) \leq 3$, then $\alpha \wedge \alpha = 0$ whenever $\alpha \in \bigwedge(V)$.

Problem 34.8. Prove Proposition 34.13.

Problem 34.9. Given two graded algebras E and F, define $E \mathbin{\widehat{\otimes}} F$ to be the vector space $E \otimes F$, but with a skew-commutative multiplication given by

$$(a \otimes b) \wedge (c \otimes d) = (-1)^{\deg(b)\deg(c)}(ac) \otimes (bd),$$

where $a \in E^m, b \in F^p$, $c \in E^n, d \in F^q$. Show that

$$\bigwedge(E \oplus F) \cong \bigwedge(E) \mathbin{\widehat{\otimes}} \bigwedge(F).$$

Problem 34.10. If $\langle -, - \rangle$ denotes the inner product on V, recall that we defined an inner product on $\bigwedge^k V$, also denoted $\langle -, - \rangle$, by setting

$$\langle u_1 \wedge \cdots \wedge u_k, v_1 \wedge \cdots \wedge v_k \rangle = \det(\langle u_i, v_j \rangle),$$

for all $u_i, v_i \in V$, and extending $\langle -, - \rangle$ by bilinearity.

Show that if $(e_1, \ldots, e_n)$ is an orthonormal basis of V, then the basis of $\bigwedge^k V$ consisting of the e_I (where $I = \{i_1, \ldots, i_k\}$, with $1 \leq i_1 < \cdots < i_k \leq n$) is also an orthonormal basis of $\bigwedge^k V$.

Problem 34.11. Show that

$$(u^* \wedge v^*) \lrcorner z = u^* \lrcorner (v^* \lrcorner z),$$

whenever $u^* \in \bigwedge^k E^*$, $v^* \in \bigwedge^{p-k} E^*$, and $z \in \bigwedge^{p+q} E$.

Problem 34.12. Prove Statement (3) of Proposition 34.18.

Problem 34.13. Prove Proposition 34.19.

Also prove the identity

$$u^* \lrcorner (x \wedge y) = (-1)^s (u^* \lrcorner x) \wedge y + x \wedge (u^* \lrcorner y),$$

where $u^* \in E^*$, $x \in \bigwedge^{q+1-s} E$, and $y \in \bigwedge^s E$.

Problem 34.14. Use the Grassmann-Plücker's equations prove that if $\dim(E) = n$, then every tensor in $\bigwedge^{n-1}(E)$ is decomposable.

Problem 34.15. Recall that the map

$$\mu_F \colon \left(\bigwedge^n (E^*)\right) \otimes F \longrightarrow \mathrm{Alt}^n(E; F)$$

is defined on generators by

$$\mu_F((v_1^* \wedge \cdots \wedge v_n^*) \otimes f)(u_1, \ldots, u_n) = (\det(v_j^*(u_i))f,$$

with $v_1^*, \ldots, v_n^* \in E^*$, $u_1, \ldots, u_n \in E$, and $f \in F$.

Given any three vector spaces, F, G, H, and any bilinear map $\Phi \colon F \times G \to H$, for all $\omega \in (\bigwedge^n(E^*)) \otimes F$ and all $\eta \in (\bigwedge^n(E^*)) \otimes G$ prove that

$$\mu_H(\omega \wedge_\Phi \eta) = \mu_F(\omega) \wedge_\Phi \mu_G(\eta).$$

Chapter 35

Introduction to Modules; Modules over a PID

35.1 Modules over a Commutative Ring

In this chapter we introduce modules over a commutative ring (with unity). After a quick overview of fundamental concepts such as free modules, torsion modules, and some basic results about them, we focus on finitely generated modules over a PID and we prove the structure theorems for this class of modules (invariant factors and elementary divisors). Our main goal is not to give a comprehensive exposition of modules, but instead to apply the structure theorem to the $K[X]$-module E_f defined by a linear map f acting on a finite-dimensional vector space E, and to obtain several normal forms for f, including the rational canonical form.

A module is the generalization of a vector space E over a field K obtained replacing the field K by a commutative ring A (with unity 1). Although formally the definition is the same, the fact that some nonzero elements of A are not invertible has some serious consequences. For example, it is possible that $\lambda \cdot u = 0$ for some nonzero $\lambda \in A$ and some nonzero $u \in E$, and a module may no longer have a basis.

For the sake of completeness, we give the definition of a module, although it is the same as Definition 3.1 with the field K replaced by a ring A. In this chapter, *all rings under consideration are assumed to be commutative and to have an identity element* 1.

Definition 35.1. Given a ring A, a *(left) module over* A (or A*-module*) is a set M (of vectors) together with two operations $+\colon M \times M \to M$ (called *vector addition*),[1] and $\cdot\colon A \times M \to M$ (called *scalar multiplication*) satisfying the following conditions for all $\alpha, \beta \in A$ and all $u, v \in M$;

(M0) M is an abelian group w.r.t. $+$, with identity element 0;

[1] The symbol $+$ is overloaded, since it denotes both addition in the ring A and addition of vectors in M. It is usually clear from the context which $+$ is intended.

(M1) $\alpha \cdot (u + v) = (\alpha \cdot u) + (\alpha \cdot v)$;

(M2) $(\alpha + \beta) \cdot u = (\alpha \cdot u) + (\beta \cdot u)$;

(M3) $(\alpha * \beta) \cdot u = \alpha \cdot (\beta \cdot u)$;

(M4) $1 \cdot u = u$.

Given $\alpha \in A$ and $v \in M$, the element $\alpha \cdot v$ is also denoted by αv. The ring A is often called the ring of scalars.

Unless specified otherwise or unless we are dealing with several different rings, in the rest of this chapter, we assume that all A-modules are defined with respect to a fixed ring A. Thus, we will refer to a A-module simply as a module.

From (M0), a module always contains the null vector 0, and thus is nonempty. From (M1), we get $\alpha \cdot 0 = 0$, and $\alpha \cdot (-v) = -(\alpha \cdot v)$. From (M2), we get $0 \cdot v = 0$, and $(-\alpha) \cdot v = -(\alpha \cdot v)$. The ring A itself can be viewed as a module over itself, addition of vectors being addition in the ring, and multiplication by a scalar being multiplication in the ring.

When the ring A is a field, an A-module is a vector space. When $A = \mathbb{Z}$, a $\mathbb{Z}$-module is just an abelian group, with the action given by

$$\begin{aligned} &0 \cdot u = 0, && \\ &n \cdot u = \underbrace{u + \cdots + u}_{n}, && n > 0 \\ &n \cdot u = -(-n) \cdot u, && n < 0. \end{aligned}$$

All definitions from Section 3.4, linear combinations, linear independence and linear dependence, subspaces renamed as *submodules*, apply unchanged to modules. Proposition 3.5 also holds for the module spanned by a set of vectors. The definition of a basis (Definition 3.6) also applies to modules, but the only result from Section 3.5 that holds for modules is Proposition 3.12. Unfortunately, it is longer true that every module has a basis. For example, for any nonzero integer $n \in \mathbb{Z}$, the $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$ has no basis since $n \cdot \overline{x} = 0$ for all $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$. Similarly, $\mathbb{Q}$, as a $\mathbb{Z}$-module, has no basis. Any two distinct nonzero elements p_1/q_1 and p_2/q_2 are linearly dependent, since

$$(p_2 q_1)\left(\frac{p_1}{q_1}\right) - (p_1 q_2)\left(\frac{p_2}{q_2}\right) = 0.$$

Furthermore, the $\mathbb{Z}$-module $\mathbb{Q}$ is not finitely generated. For if $\{p_1/q_1, \cdots p_n/q_n\} \subset \mathbb{Q}$ generated $\mathbb{Q}$, then for any $x = r/s \in \mathbb{Q}$, we have

$$c_1 \frac{p_1}{q_1} + \cdots + c_n \frac{p_n}{q_n} = \frac{r}{s},$$

where $c_i \in \mathbb{Z}$ for $i = 1, \ldots, n$. The left hand side of the preceding line is equivalent to

$$\frac{c_1 p_1 q_2 \cdots q_n + \cdots + c_n p_n q_1 \cdots q_{n-1}}{q_1 q_2 \cdots q_n},$$

where the numerator is an element of the ideal in $\mathbb{Z}$ spanned by $(c_1, c_2, \cdots, c_n)$. Since $\mathbb{Z}$ is a PID, there exists $a \in \mathbb{Z}$ such that (a) is the ideal spanned by $(c_1, c_2, \cdots, c_n)$. Thus

$$c_1 \frac{p_1}{q_1} + \cdots + c_n \frac{p_n}{q_n} = \frac{ma}{q_1 q_2 \cdots q_n} = \frac{r}{s},$$

where $m \in \mathbb{Z}$. Set

$$\frac{a}{q_1 q_2 \cdots q_n} = \frac{a_1}{b}, \qquad (a_1, b) = 1.$$

Then if $\mathbb{Q}$ was a finitely generated $\mathbb{Z}$-module, we deduce that for all $x \in \mathbb{Q}$

$$x = \frac{r}{s} = m \frac{a_1}{b},$$

whenever a_1/b is a fixed rational number, clearly a contradiction. (In particular let $x = 1/p$ where p is a fixed prime $p > b$. If $ma_1/b = 1/p$, then $ma_1 \in \mathbb{Z}$ with $ma_1 = b_1/p$, an impossiblity since $(b_1, p) = 1$ and $p > b_1$.)

Definition 3.11 can be generalized to rings and yields free modules.

Definition 35.2. Given a commutative ring A and any (nonempty) set I, let $A^{(I)}$ be the subset of the cartesian product A^I consisting of all families $(\lambda_i)_{i \in I}$ with finite support of scalars in A.[2] We define addition and multiplication by a scalar as follows:

$$(\lambda_i)_{i \in I} + (\mu_i)_{i \in I} = (\lambda_i + \mu_i)_{i \in I},$$

and

$$\lambda \cdot (\mu_i)_{i \in I} = (\lambda \mu_i)_{i \in I}.$$

It is immediately verified that addition and multiplication by a scalar are well defined. Thus, $A^{(I)}$ is a module. Furthermore, because families with finite support are considered, the family $(e_i)_{i \in I}$ of vectors e_i, defined such that $(e_i)_j = 0$ if $j \neq i$ and $(e_i)_i = 1$, is clearly a basis of the module $A^{(I)}$. When $I = \{1, \ldots, n\}$, we denote $A^{(I)}$ by A^n. The function $\iota \colon I \to A^{(I)}$, such that $\iota(i) = e_i$ for every $i \in I$, is clearly an injection.

Definition 35.3. An A-module M is *free* iff it has a basis.

The module $A^{(I)}$ is a free module.

All definitions from Section 3.7 apply to modules, linear maps, kernel, image, except the definition of rank, which has to be defined differently. Propositions 3.14, 3.15, 3.16, and

[2] Where A^I denotes the set of all functions from I to A.

3.17 hold for modules. However, the other propositions do not generalize to modules. The definition of an isomorphism generalizes to modules. As a consequence, a module is free iff it is isomorphic to a module of the form $A^{(I)}$.

Section 3.8 generalizes to modules. Given a submodule N of a module M, we can define the quotient module M/N.

If $\mathfrak{a}$ is an ideal in A and if M is an A-module, we define $\mathfrak{a}M$ as the set of finite sums of the form

$$a_1m_1 + \cdots + a_km_k, \quad a_i \in \mathfrak{a},\ m_i \in M.$$

It is immediately verified that $\mathfrak{a}M$ is a submodule of M.

Interestingly, the part of Theorem 3.11 that asserts that any two bases of a vector space have the same cardinality holds for modules. One way to prove this fact is to "pass" to a vector space by a quotient process.

Theorem 35.1. *For any free module M, any two bases of M have the same cardinality.*

Proof sketch. We give the argument for finite bases, but it also holds for infinite bases. The trick is to pick any maximal ideal $\mathfrak{m}$ in A (whose existence is guaranteed by Theorem B.3). Then, $A/\mathfrak{m}$ is a field, and $M/\mathfrak{m}M$ can be made into a vector space over $A/\mathfrak{m}$; we leave the details as an exercise. If $(u_1, \ldots, u_n)$ is a basis of M, then it is easy to see that the image of this basis is a basis of the vector space $M/\mathfrak{m}M$. By Theorem 3.11, the number n of elements in any basis of $M/\mathfrak{m}M$ is an invariant, so any two bases of M must have the same number of elements. □

Definition 35.4. The common number of elements in any basis of a free module is called the *dimension* (or *rank*) of the free module.

One should realize that the notion of linear independence in a module is a little tricky. According to the definition, the one-element sequence (u) consisting of a single nonzero vector is linearly independent if for all $\lambda \in A$, if $\lambda u = 0$ then $\lambda = 0$. However, there are free modules that contain nonzero vectors that are not linearly independent! For example, the ring $A = \mathbb{Z}/6\mathbb{Z}$ viewed as a module over itself has the basis (1), but the zero-divisors, such as 2 or 4, are not linearly independent. Using language introduced in Definition 35.5, a free module may have torsion elements. There are also nonfree modules such that every nonzero vector is linearly independent, such as $\mathbb{Q}$ over $\mathbb{Z}$.

All definitions from Section 4.1 about matrices apply to free modules, and so do all the propositions. Similarly, all definitions from Section 6.1 about direct sums and direct products apply to modules. All propositions that do not involve extending bases still hold. The important Proposition 6.12 survives in the following form.

Proposition 35.2. *Let $f \colon E \to F$ be a surjective linear map between two A-modules with F a free module. Given any basis $(v_1, \ldots, v_r)$ of F, for any r vectors $u_1, \ldots, u_r \in E$ such that $f(u_i) = v_i$ for $i = 1, \ldots, r$, the vectors $(u_1, \ldots, u_r)$ are linearly independent and the module E is the direct sum*

$$E = \mathrm{Ker}\,(f) \oplus U,$$

where U is the free submodule of E spanned by the basis $(u_1, \ldots, u_r)$.

Proof. Pick any $w \in E$, write $f(w)$ over the basis $(v_1, \ldots, v_r)$ as $f(w) = a_1v_1 + \cdots + a_rv_r$, and let $u = a_1u_1 + \cdots + a_ru_r$. Observe that

$$\begin{aligned} f(w-u) &= f(w) - f(u) \\ &= a_1v_1 + \cdots + a_rv_r - (a_1f(u_1) + \cdots + a_rf(u_r)) \\ &= a_1v_1 + \cdots + a_rv_r - (a_1v_1 + \cdots + a_rv_r) \\ &= 0. \end{aligned}$$

Therefore, $h = w - u \in \mathrm{Ker}\,(f)$, and since $w = h + u$ with $h \in \mathrm{Ker}\,(f)$ and $u \in U$, we have $E = \mathrm{Ker}\,(f) + U$.

If $u = a_1u_1 + \cdots + a_ru_r \in U$ also belongs to $\mathrm{Ker}\,(f)$, then

$$0 = f(u) = f(a_1u_1 + \cdots + a_ru_r) = a_1v_1 + \cdots + a_rv_r,$$

and since $(v_1, \ldots, v_r)$ is a basis, $a_i = 0$ for $i = 1, \ldots, r$, which shows that $\mathrm{Ker}\,(f) \cap U = (0)$. Therefore, we have a direct sum

$$E = \mathrm{Ker}\,(f) \oplus U.$$

Finally, if

$$a_1u_1 + \cdots + a_ru_r = 0,$$

the above reasoning shows that $a_i = 0$ for $i = 1, \ldots, r$, so $(u_1, \ldots, u_r)$ are linearly independent. Therefore, the module U is a free module. □

One should be aware that if we have a direct sum of modules

$$U = U_1 \oplus \cdots \oplus U_m,$$

every vector $u \in U$ can be written is a unique way as

$$u = u_1 + \cdots + u_m,$$

with $u_i \in U_i$ but, unlike the case of vector spaces, this does not imply that any m nonzero vectors $(u_1, \ldots, u_m)$ are linearly independent. For example, we have the direct sum

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

where $\mathbb{Z}/2\mathbb{Z}$ is viewed as a $\mathbb{Z}$-modules, but $(1, 0)$ and $(0, 1)$ are not linearly independent, since

$$2(1, 0) + 2(0, 1) = (0, 0).$$

A useful fact is that every module is a quotient of some free module. Indeed, if M is an A-module, pick any spanning set I for M (such a set exists, for example, $I = M$), and consider the unique homomorphism $\varphi\colon A^{(I)} \to M$ extending the identity function from I to itself. Then we have an isomorphism $A^{(I)}/\mathrm{Ker}\,(\varphi) \approx M$.

In particular, if M is finitely generated, we can pick I to be a finite set of generators, in which case we get an isomorphism $A^n/\mathrm{Ker}\,(\varphi) \approx M$, for some natural number n. A finitely generated module is sometimes called a module of *finite type*.

The case $n = 1$ is of particular interest. A module M is said to be *cyclic* if it is generated by a single element. In this case $M = Ax$, for some $x \in M$. We have the linear map $m_x\colon A \to M$ given by $a \mapsto ax$ for every $a \in A$, and it is obviously surjective since $M = Ax$. Since the kernel $\mathfrak{a} = \mathrm{Ker}\,(m_x)$ of m_x is an ideal in A, we get an isomorphism $A/\mathfrak{a} \approx Ax$. Conversely, for any ideal $\mathfrak{a}$ of A, if $M = A/\mathfrak{a}$, we see that M is generated by the image x of 1 in M, so M is a cyclic module.

The ideal $\mathfrak{a} = \mathrm{Ker}\,(m_x)$ is the set of all $a \in A$ such that $ax = 0$. This is called the *annihilator* of x, and it is the special case of the following more general situation.

Definition 35.5. If M is any A-module, for any subset S of M, the set of all $a \in A$ such that $ax = 0$ for all $x \in S$ is called the *annihilator* of S, and it is denoted by $\mathrm{Ann}(S)$. If $S = \{x\}$, we write $\mathrm{Ann}(x)$ instead of $\mathrm{Ann}(\{x\})$. A nonzero element $x \in M$ is called a *torsion element* iff $\mathrm{Ann}(x) \neq (0)$. The set consisting of all torsion elements in M and 0 is denoted by M_{tor}.

It is immediately verified that $\mathrm{Ann}(S)$ is an ideal of A, and by definition,

$$M_{\mathrm{tor}} = \{x \in M \mid (\exists a \in A,\ a \neq 0)(ax = 0)\}.$$

If a ring has zero divisors, then the set of all torsion elements in an A-module M may not be a submodule of M. For example, if $M = A = \mathbb{Z}/6\mathbb{Z}$, then $M_{\mathrm{tor}} = \{2, 3, 4\}$, but $3 + 4 = 1$ is not a torsion element. Also, a free module may not be torsion-free because there may be torsion elements, as the example of $\mathbb{Z}/6\mathbb{Z}$ as a free module over itself shows.

However, if A is an integral domain, then a free module is torsion-free and M_{tor} is a submodule of M. (Recall that an integral domain is commutative).

Proposition 35.3. *If A is an integral domain, then for any A-module M, the set M_{tor} of torsion elements in M is a submodule of M.*

Proof. If $x, y \in M$ are torsion elements $(x, y \neq 0)$, then there exist some nonzero elements $a, b \in A$ such that $ax = 0$ and $by = 0$. Since A is an integral domain, $ab \neq 0$, and then for all $\lambda, \mu \in A$, we have

$$ab(\lambda x + \mu y) = b\lambda ax + a\mu by = 0.$$

Therefore, M_{tor} is a submodule of M. □

The module M_{tor} is called the *torsion submodule* of M. If $M_{\text{tor}} = (0)$, then we say that M is *torsion-free*, and if $M = M_{\text{tor}}$, then we say that M is a *torsion module*.

If M is not finitely generated, then it is possible that $M_{\text{tor}} \neq 0$, yet the annihilator of M_{tor} is reduced to 0. For example, let take the $\mathbb{Z}$-module

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z} \times \cdots ,$$

where p ranges over the set of primes. Call this module M and the set of primes P. Observe that M is generated by $\{\alpha_p\}_{p\in P}$, where α_p is the tuple whose only nonzero entry is $\overline{1}_p$, the generator of $\mathbb{Z}/p\mathbb{Z}$, i.e.,

$$\alpha_p = (\overline{0}, \overline{0}, \overline{0}, \cdots , \overline{1}_p, \overline{0}, \cdots), \qquad \mathbb{Z}/p\mathbb{Z} = \{n \cdot \overline{1}_p\}_{n=0}^{p-1}.$$

In other words, M is not finitely generated. Furthermore, since $p \cdot \overline{1}_p = \overline{0}$, we have $\{\alpha_p\}_{p\in P} \subset M_{\text{tor}}$. However, because p ranges over all primes, the only possible nonzero annihilator of $\{\alpha_p\}_{p\in P}$ would be the product of all the primes. Hence $\text{Ann}(\{\alpha_p\}_{p\in P}) = (0)$. Because of the subset containment, we conclude that $\text{Ann}(M_{\text{tor}}) = (0)$.

However, if M is finitely generated, it is *not* possible that $M_{\text{tor}} \neq 0$, yet the annihilator of M_{tor} is reduced to 0, since if $x_1, \ldots, x_n$ generate M and if $a_1, \ldots, a_n$ annihilate $x_1, \ldots, x_n$, then $a_1 \cdots a_n$ annihilates every element of M.

Proposition 35.4. *If A is an integral domain, then for any A-module M, the quotient module M/M_{tor} is torsion free.*

Proof. Let $\overline{x}$ be an element of M/M_{tor} and assume that $a\overline{x} = 0$ for some $a \neq 0$ in A. This means that $ax \in M_{\text{tor}}$, so there is some $b \neq 0$ in A such that $bax = 0$. Since $a, b \neq 0$ and A is an integral domain, $ba \neq 0$, so $x \in M_{\text{tor}}$, which means that $\overline{x} = 0$. □

If A is an integral domain and if F is a free A-module with basis $(u_1, \ldots, u_n)$, then F can be embedded in a K-vector space F_K isomorphic to K^n, where $K = \text{Frac}(A)$ is the fraction field of A. Similarly, any submodule M of F is embedded into a subspace M_K of F_K. Note that any linearly independent vectors $(u_1, \ldots, u_m)$ in the A-module M remain linearly independent in the vector space M_K, because any linear dependence over K is of the form

$$\frac{a_1}{b_1}\, u_1 + \cdots + \frac{a_m}{b_m}\, u_m = 0$$

for some $a_i, b_i \in A$, with $b_1 \cdots b_m \neq 0$, so if we multiply by $b_1 \cdots b_m \neq 0$, we get a linear dependence in the A-module M. Then we see that the maximum number of linearly independent vectors in the A-module M is at most n. The maximum number of linearly independent vectors in a finitely generated submodule of a free module (over an integral domain) is called the *rank* of the module M. If $(u_1, \ldots, u_m)$ are linearly independent where

m is the rank of m, then for every nonzero $v \in M$, there are some $a, a_1, \ldots, a_m \in A$, not all zero, such that

$$av = a_1u_1 + \cdots + a_mu_m.$$

We must have $a \neq 0$, since otherwise, linear independence of the u_i would imply that $a_1 = \cdots = a_m = 0$, contradicting the fact that $a, a_1, \ldots, a_m \in A$ are not all zero.

Unfortunately, in general, a torsion-free module is not free. For example, $\mathbb{Q}$ as a $\mathbb{Z}$-module is torsion-free but not free. If we restrict ourselves to finitely generated modules over PID's, then such modules split as the direct sum of their torsion module with a free module, and a torsion module has a nice decomposition in terms of cyclic modules.

The following proposition shows that over a PID, submodules of a free module are free. There are various ways of proving this result. We give a proof due to Lang [108] (see Chapter III, Section 7).

Proposition 35.5. *If A is a PID and if F is a free A-module of dimension n, then every submodule M of F is a free module of dimension at most n.*

Proof. Let $(u_1, \ldots, u_n)$ be a basis of F, and let $M_r = M \cap (Au_1 \oplus \cdots \oplus Au_r)$, the intersection of M with the free module generated by $(u_1, \ldots, u_r)$, for $r = 1, \ldots, n$. We prove by induction on r that each M_r is free and of dimension at most r. Since $M = M_r$ for some r, this will prove our result.

Consider $M_1 = M \cap Au_1$. If $M_1 = (0)$, we are done. Otherwise let

$$\mathfrak{a} = \{a \in A \mid au_1 \in M\}.$$

It is immediately verified that $\mathfrak{a}$ is an ideal, and since A is a PID, $\mathfrak{a} = a_1A$, for some $a_1 \in A$. Since we are assuming that $M_1 \neq (0)$, we have $a_1 \neq 0$, and $a_1u_1 \in M$. If $x \in M_1$, then $x = au_1$ for some $a \in A$, so $a \in a_1A$, and thus $a = ba_1$ for some $b \in A$. It follows that $M_1 = Aa_1u_1$, which is free.

Assume inductively that M_r is free of dimension at most $r < n$, and let

$$\mathfrak{a} = \{a \in A \mid (\exists b_1 \in A) \cdots (\exists b_r \in A)(b_1u_1 + \cdots + b_ru_r + au_{r+1} \in M)\}.$$

It is immediately verified that $\mathfrak{a}$ is an ideal, and since A is a PID, $\mathfrak{a} = a_{r+1}A$, for some $a_{r+1} \in A$. If $a_{r+1} = 0$, then $M_{r+1} = M_r$, and we are done.

If $a_{r+1} \neq 0$, then there is some $v_1 \in Au_1 \oplus \cdots \oplus Au_r$ such that

$$w = v_1 + a_{r+1}u_{r+1} \in M.$$

For any $x \in M_{r+1}$, there is some $v \in Au_1 \oplus \cdots \oplus Au_r$ and some $a \in A$ such that $x = v + au_{r+1}$. Then, $a \in a_{r+1}A$, so there is some $b \in A$ such that $a = ba_{r+1}$. As a consequence

$$x - bw = v - bv_1 \in M_r,$$

and so $x = x - bw + bw$ with $x - bw \in M_r$, which shows that

$$M_{r+1} = M_r + Aw.$$

On the other hand, if $u \in M_r \cap Aw$, then since $w = v_1 + a_{r+1}u_{r+1}$ we have

$$u = bv_1 + ba_{r+1}u_{r+1},$$

for some $b \in A$, with $u, v_1 \in Au_1 \oplus \cdots \oplus Au_r$, and if $b \neq 0$, this yields the nontrivial linear combination

$$bv_1 - u + ba_{r+1}u_{r+1} = 0,$$

contradicting the fact that $(u_1, \ldots, u_{r+1})$ are linearly independent. Therefore,

$$M_{r+1} = M_r \oplus Aw,$$

which shows that M_{r+1} is free of dimension at most $r + 1$. □

The following two examples show why the hypothesis of Proposition 35.5 requires A to be PID. First consider $6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ as a free $6\mathbb{Z}$-module with generator $\overline{1}$. The $6\mathbb{Z}$-submodule $\{\overline{0}, \overline{2}, \overline{4}\}$ is not free, even though it is generated by $\overline{2}$ since $\overline{3} \cdot \overline{2} = \overline{0}$. Proposition 35.5 fails since $6\mathbb{Z}$ is not even an integral domain. Next consider $\mathbb{Z}[X]$ as a free $\mathbb{Z}[X]$-module with generator 1. We claim the ideal

$$(2, X) = \{2p(X) + Xq(X) \mid p(X), q(X) \in \mathbb{Z}[X]\},$$

is not a free $\mathbb{Z}[X]$-module. Indeed any two nonzero elements of $(2, X)$, say $s(X)$ and $t(X)$, are linearly dependent since $t(X)s(X) - s(X)t(X) = 0$. Once again Proposition 35.5 fails since $\mathbb{Z}[X]$ is not a PID. See Example 32.1.

Proposition 35.5 implies that if M is a finitely generated module over a PID, then any submodule N of M is also finitely generated.

Indeed, if $(u_1, \ldots, u_n)$ generate M, then we have a surjection $\varphi\colon A^n \to M$ from the free module A^n onto M. The inverse image $\varphi^{-1}(N)$ of N is a submodule of the free module A^n, therefore by Proposition 35.5, $\varphi^{-1}(N)$ is free and finitely generated. This implies that N is finitely generated (and that it has a number of generators $\leq n$).

We can also prove that a finitely generated torsion-free module over a PID is actually free. We will give another proof of this fact later, but the following proof is instructive.

Proposition 35.6. *If A is a PID and if M is a finitely generated module which is torsion-free, then M is free.*

Proof. Let $(y_1, \ldots, y_n)$ be some generators for M, and let $(u_1, \ldots, u_m)$ be a maximal subsequence of $(y_1, \ldots, y_n)$ which is linearly independent. If $m = n$, we are done. Otherwise, due to the maximality of m, for $i = 1, \ldots, n$, there is some $a_i \neq 0$ such that such that

$a_i y_i$ can be expressed as a linear combination of $(u_1, \ldots, u_m)$. If we let $a = a_1 \ldots a_n$, then $a_1 \ldots a_n y_i \in Au_1 \oplus \cdots \oplus Au_m$ for $i = 1, \ldots, n$, which shows that

$$aM \subseteq Au_1 \oplus \cdots \oplus Au_m.$$

Now, A is an integral domain, and since $a_i \neq 0$ for $i = 1, \ldots, n$, we have $a = a_1 \ldots a_n \neq 0$, and because M is torsion-free, the map $x \mapsto ax$ is injective. It follows that M is isomorphic to a submodule of the free module $Au_1 \oplus \cdots \oplus Au_m$. By Proposition 35.5, this submodule if free, and thus, M is free. □

Although we will obtain this result as a corollary of the structure theorem for finitely generated modules over a PID, we are in the position to give a quick proof of the following theorem.

Theorem 35.7. *Let M be a finitely generated module over a PID. Then M/M_{tor} is free, and there exit a free submodule F of M such that M is the direct sum*

$$M = M_{\mathrm{tor}} \oplus F.$$

The dimension of F is uniquely determined.

Proof. By Proposition 35.4 M/M_{tor} is torsion-free, and since M is finitely generated, it is also finitely generated. By Proposition 35.6, M/M_{tor} is free. We have the quotient linear map $\pi\colon M \to M/M_{\mathrm{tor}}$, which is surjective, and M/M_{tor} is free, so by Proposition 35.2, there is a free module F isomorphic to M/M_{tor} such that

$$M = \mathrm{Ker}\,(\pi) \oplus F = M_{\mathrm{tor}} \oplus F.$$

Since F is isomorphic to M/M_{tor}, the dimension of F is uniquely determined. □

Theorem 35.7 reduces the study of finitely generated module over a PID to the study of finitely generated torsion modules. This is the path followed by Lang [108] (Chapter III, section 7).

35.2 Finite Presentations of Modules

Since modules are generally not free, it is natural to look for techniques for dealing with nonfree modules. The hint is that if M is an A-module and if $(u_i)_{i\in I}$ is any set of generators for M, then we know that there is a surjective homomorphism $\varphi\colon A^{(I)} \to M$ from the free module $A^{(I)}$ generated by I onto M. Furthermore M is isomorphic to $A^{(I)}/\mathrm{Ker}\,(\varphi)$. Then, we can pick a set of generators $(v_j)_{j\in J}$ for $\mathrm{Ker}\,(\varphi)$, and again there is a surjective map $\psi\colon A^{(J)} \to \mathrm{Ker}\,(\varphi)$ from the free module $A^{(J)}$ generated by J onto $\mathrm{Ker}\,(\varphi)$. The map ψ can be viewed a linear map from $A^{(J)}$ to $A^{(I)}$, we have

$$\mathrm{Im}(\psi) = \mathrm{Ker}\,(\varphi),$$

and φ is surjective. Note that M is isomorphic to $A^{(I)}/\mathrm{Im}(\psi)$. In such a situation we say that we have an *exact sequence* and this is denoted by the diagram

$$\begin{tikzcd} A^{(J)} \arrow[r, "\psi"] & A^{(I)} \arrow[r, "\varphi"] & M \arrow[r] & 0. \end{tikzcd}$$

Definition 35.6. Given an A-module M, a *presentation* of M is an exact sequence

$$\begin{tikzcd} A^{(J)} \arrow[r, "\psi"] & A^{(I)} \arrow[r, "\varphi"] & M \arrow[r] & 0 \end{tikzcd}$$

which means that

1. $\mathrm{Im}(\psi) = \mathrm{Ker}\,(\varphi)$.

2. φ is surjective.

Consequently, M is isomorphic to $A^{(I)}/\mathrm{Im}(\psi)$. If I and J are both finite, we say that this is a *finite presentation* of M.

Observe that in the case of a finite presentation, I and J are finite, and if $|J| = n$ and $|I| = m$, then ψ is a linear map $\psi\colon A^n \to A^m$, so it is given by some $m \times n$ matrix R with coefficients in A called the *presentation matrix* of M. Every column R^j of R may thought of as a relation

$$a_{j1}e_1 + \cdots + a_{jm}e_m = 0$$

among the generators $e_1, \ldots, e_m$ of A^m, so we have n relations among these generators. Also the images of $e_1, \ldots, e_m$ in M are generators of M, so we can think of the above relations as relations among the generators of M.

The submodule of A^m spanned by the columns of R is *the set of relations* of M, and the columns of R are called a *complete set of relations* for M. The vectors $e_1, \ldots, e_m$ are called a set of *generators* for M. We may also say that the generators $e_1, \ldots, e_m$ and the relations $R^1, \ldots, R^n$ (the columns of R) are a (finite) presentation of the module M. The *module M presented by R is isomorphic to A^m/RA^n*, where we denote by RA^n the image of A^n by the linear map defined by R.

For example, the $\mathbb{Z}$-module presented by the 1×1 matrix $R = (5)$ is the quotient, $\mathbb{Z}/5\mathbb{Z}$, of $\mathbb{Z}$ by the submodule $5\mathbb{Z}$ corresponding to the single relation

$$5e_1 = 0.$$

But $\mathbb{Z}/5\mathbb{Z}$ has other presentations. For example, if we consider the matrix of relations

$$R = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix},$$

presenting the module M, then we have the relations

$$\begin{aligned} 2e_1 + e_2 &= 0 \\ -e_1 + 2e_2 &= 0. \end{aligned}$$

From the first equation, we get $e_2 = -2e_1$, and substituting into the second equation we get

$$-5e_1 = 0.$$

It follows that the generator e_2 can be eliminated and M is generated by the single generator e_1 satisfying the relation

$$5e_1 = 0,$$

which shows that $M \approx \mathbb{Z}/5\mathbb{Z}$.

The above example shows that many different matrices can present the same module. Here are some useful rules for manipulating a relation matrix without changing the isomorphism class of the module M it presents.

Proposition 35.8. *If R is an $m \times n$ matrix presenting an A-module M, then the matrices S of the form listed below present the same module (a module isomorphic to M):*

(1) $S = QRP^{-1}$, where Q is a $m \times m$ invertible matrix and P a $n \times n$ invertible matrix (both over A).

(2) S is obtained from R by deleting a column of zeros.

(3) The jth column of R is e_i, and S is obtained from R by deleting the ith row and the jth column.

Proof. (1) By definition, we have an isomorphism $M \approx A^m/RA^n$, where we denote by RA^n the image of A^n by the linear map defined by R. Going from R to QRP^{-1} corresponds to making a change of basis in A^m and a change of basis in A^n, and this yields a quotient module isomorphic to M.

(2) A zero column does not contribute to the span of the columns of R, so it can be eliminated.

(3) If the jth column of R is e_i, then when taking the quotient A^m/RA^n, the generator e_i goes to zero. This means that the generator e_i is redundant, and when we delete it, we get a matrix of relations in which the ith row of R and the jth column of R are deleted. □

The matrices P and Q are often products of elementary operations. One should be careful that rows of zeros cannnot be eliminated. For example, the 2×1 matrix

$$R_1 = \begin{pmatrix} 4 \\ 0 \end{pmatrix}$$

gives the single relation

$$4e_1 = 0,$$

but the second generator e_2 cannot be eliminated. This matrix presents the module $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}$. On the other hand, the 1×2 matrix

$$R_2 = \begin{pmatrix} 4 & 0 \end{pmatrix}$$

gives two relations

$$\begin{aligned} 4e_1 &= 0, \\ 0 &= 0, \end{aligned}$$

so the second generator can be eliminated and R_2 presents the module $\mathbb{Z}/4\mathbb{Z}$.

The rules of Proposition 35.8 make it possible to simplify a presentation matrix quite a lot in some cases. For example, consider the relation matrix

$$R = \begin{pmatrix} 3 & 8 & 7 & 9 \\ 2 & 4 & 6 & 6 \\ 1 & 2 & 2 & 1 \end{pmatrix}.$$

By subtracting 2 times row 3 from row 2 and subtracting 3 times row 3 from row 1, we get

$$\begin{pmatrix} 0 & 2 & 1 & 6 \\ 0 & 0 & 2 & 4 \\ 1 & 2 & 2 & 1 \end{pmatrix}.$$

After deleting column 1 and row 3, we get

$$\begin{pmatrix} 2 & 1 & 6 \\ 0 & 2 & 4 \end{pmatrix}.$$

By subtracting 2 times row 1 from row 2, we get

$$\begin{pmatrix} 2 & 1 & 6 \\ -4 & 0 & -8 \end{pmatrix}.$$

After deleting column 2 and row 1, we get

$$\begin{pmatrix} -4 & -8 \end{pmatrix}.$$

By subtracting 2 times column 1 from column 2, we get

$$\begin{pmatrix} -4 & 0 \end{pmatrix}.$$

Finally, we can drop the second column and we get

$$(4),$$

which shows that R presents the module $\mathbb{Z}/4\mathbb{Z}$.

Unfortunately a submodule of a free module of finite dimension is not necessarily finitely generated but, by Proposition 35.5, if A is a PID, then any submodule of a finitely generated module is finitely generated. This property actually characterizes Noetherian rings. To prove it, we need a slightly different version of Proposition 35.2.

Proposition 35.9. *Let $f\colon E \to F$ be a linear map between two A-modules E and F.*

(1) Given any set of generators $(v_1, \ldots, v_r)$ of $\mathrm{Im}(f)$, for any r vectors $u_1, \ldots, u_r \in E$ such that $f(u_i) = v_i$ for $i = 1, \ldots, r$, if U is the finitely generated submodule of E generated by $(u_1, \ldots, u_r)$, then the module E is the sum

$$E = \mathrm{Ker}\,(f) + U.$$

Consequently, if both $\mathrm{Ker}\,(f)$ and $\mathrm{Im}(f)$ are finitely generated, then E is finitely generated.

(2) If E is finitely generated, then so is $\mathrm{Im}(f)$.

Proof. (1) Pick any $w \in E$, write $f(w)$ over the generators $(v_1, \ldots, v_r)$ of $\mathrm{Im}(f)$ as $f(w) = a_1v_1 + \cdots + a_rv_r$, and let $u = a_1u_1 + \cdots + a_ru_r$. Observe that

$$\begin{aligned} f(w-u) &= f(w) - f(u) \\ &= a_1v_1 + \cdots + a_rv_r - (a_1f(u_1) + \cdots + a_rf(u_r)) \\ &= a_1v_1 + \cdots + a_rv_r - (a_1v_1 + \cdots + a_rv_r) \\ &= 0. \end{aligned}$$

Therefore, $h = w - u \in \mathrm{Ker}\,(f)$, and since $w = h + u$ with $h \in \mathrm{Ker}\,(f)$ and $u \in U$, we have $E = \mathrm{Ker}\,(f) + U$, as claimed. If $\mathrm{Ker}\,(f)$ is also finitely generated, by taking the union of a finite set of generators for $\mathrm{Ker}\,(f)$ and $(v_1, \ldots, v_r)$, we obtain a finite set of generators for E.

(2) If $(u_1, \ldots, u_n)$ generate E, it is obvious that $(f(u_1), \ldots, f(u_n))$ generate $\mathrm{Im}(f)$. □

Theorem 35.10. *A ring A is Noetherian iff every submodule N of a finitely generated A-module M is itself finitely generated.*

Proof. First, assume that every submodule N of a finitely generated A-module M is itself finitely generated. The ring A is a module over itself and it is generated by the single element 1. Furthermore, every submodule of A is an ideal, so the hypothesis implies that every ideal in A is finitely generated, which shows that A is Noetherian.

Now, assume A is Noetherian. First, observe that it is enough to prove the theorem for the finitely generated free modules A^n (with $n \geq 1$). Indeed, assume that we proved for every $n \geq 1$ that every submodule of A^n is finitely generated. If M is any finitely generated A-module, then there is a surjection $\varphi\colon A^n \to M$ for some n (where n is the number of elements of a finite generating set for M). Given any submodule N of M, $L = \varphi^{-1}(N)$ is a submodule of A^n. Since A^n is finitely generated, the submodule N of A^n is finitely generated, and then $N = \varphi(L)$ is finitely generated.

It remains to prove the theorem for $M = A^n$. We proceed by induction on n. For $n = 1$, a submodule N of A is an ideal, and since A is Noetherian, N is finitely generated. For the induction step where $n > 1$, consider the projection $\pi\colon A^n \to A^{n-1}$ given by

$$\pi(a_1, \ldots, a_n) = (a_1, \ldots, a_{n-1}).$$

The kernel of π is the module

$$\mathrm{Ker}\,(\pi) = \{(0, \ldots, 0, a_n) \in A^n \mid a_n \in A\} \approx A.$$

For any submodule N of A^n, let $\varphi\colon N \to A^{n-1}$ be the restriction of π to N. Since $\varphi(N)$ is a submodule of A^{n-1}, by the induction hypothesis, $\mathrm{Im}(\varphi) = \varphi(N)$ is finitely generated. Also, $\mathrm{Ker}\,(\varphi) = N \cap \mathrm{Ker}\,(\pi)$ is a submodule of $\mathrm{Ker}\,(\pi) \approx A$, and thus $\mathrm{Ker}\,(\varphi)$ is isomorphic to an ideal of A, and thus is finitely generated (since A is Noetherian). Since both $\mathrm{Im}(\varphi)$ and $\mathrm{Ker}\,(\varphi)$ are finitely generated, by Proposition 35.9, the submodule N is also finitely generated. □

As a consequence of Theorem 35.10, every finitely generated A-module over a Noetherian ring A is finitely presented, because if $\varphi\colon A^n \to M$ is a surjection onto the finitely generated module M, then $\mathrm{Ker}\,(\varphi)$ is finitely generated. In particular, if A is a PID, then every finitely generated module is finitely presented.

If the ring A is not Noetherian, then there exist finitely generated A-modules that are not finitely presented. This is not so easy to prove.

We will prove in Proposition 35.35 that if A is a PID then a matrix R can "diagonalized" as

$$R = QDP^{-1}$$

where D is a diagonal matrix (more computational versions of this proposition are given in Theorem 36.18 and Theorem 36.21). It follows from Proposition 35.8 that every finitely generated module M over a PID has a presentation with m generators and r relations of the form

$$\alpha_i e_i = 0,$$

where $\alpha_i \neq 0$ and $\alpha_1 \mid \alpha_2 \mid \cdots \mid \alpha_r$, which shows that M is isomorphic to the direct sum

$$M \approx A^{m-r} \oplus A/(\alpha_1 A) \oplus \cdots \oplus A/(\alpha_r A).$$

This is a version of Theorem 35.25 that will be proved in Section 35.5.

35.3 Tensor Products of Modules over a Commutative Ring

It is possible to define tensor products of modules over a ring, just as in Section 33.2, and the results of this section continue to hold. The results of Section 33.4 also continue to hold since they are based on the universal mapping property. However, the results of Section 33.3 on bases generally fail, except for free modules. Similarly, the results of Section 33.5 on duality generally fail. Tensor algebras can be defined for modules, as in Section 33.6. Symmetric tensor and alternating tensors can be defined for modules but again, results involving bases generally fail.

Tensor products of modules have some unexpected properties. For example, if p and q are relatively prime integers, then

$$\mathbb{Z}/p\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/q\mathbb{Z} = (0).$$

This is because, by Bezout's identity, there are $a, b \in \mathbb{Z}$ such that

$$ap + bq = 1,$$

so, for all $x \in \mathbb{Z}/p\mathbb{Z}$ and all $y \in \mathbb{Z}/q\mathbb{Z}$, we have

$$\begin{aligned} x \otimes y &= ap(x \otimes y) + bq(x \otimes y) \\ &= a(px \otimes y) + b(x \otimes qy) \\ &= a(0 \otimes y) + b(x \otimes 0) \\ &= 0. \end{aligned}$$

It is possible to salvage certain properties of tensor products holding for vector spaces by restricting the class of modules under consideration. For example, *projective modules* have a pretty good behavior w.r.t. tensor products.

A free A-module F, is a module that has a basis (*i.e.*, there is a family, $(e_i)_{i\in I}$, of linearly independent vectors in F that span F). Projective modules have many equivalent characterizations. Here is one that is best suited for our needs:

Definition 35.7. An A-module, P, is *projective* if it is a summand of a free module, that is, if there is a free A-module, F, and some A-module, Q, so that

$$F = P \oplus Q.$$

Given any A-module, M, we let $M^* = \mathrm{Hom}_A(M, A)$ be its *dual*. We have the following proposition:

Proposition 35.11. *For any finitely-generated projective A-modules, P, and any A-module, Q, we have the isomorphisms:*

$$\begin{aligned} P^{**} &\cong P \\ \mathrm{Hom}_A(P, Q) &\cong P^* \otimes_A Q. \end{aligned}$$

Proof sketch. We only consider the second isomorphism. Since P is projective, we have some A-modules, P_1, F, with

$$P \oplus P_1 = F,$$

where F is some free module. Now, we know that for any A-modules, U, V, W, we have

$$\mathrm{Hom}_A(U \oplus V, W) \cong \mathrm{Hom}_A(U, W) \coprod \mathrm{Hom}_A(V, W) \cong \mathrm{Hom}_A(U, W) \oplus \mathrm{Hom}_A(V, W),$$

so

$$P^* \oplus P_1^* \cong F^*, \qquad \mathrm{Hom}_A(P, Q) \oplus \mathrm{Hom}_A(P_1, Q) \cong \mathrm{Hom}_A(F, Q).$$

By tensoring with Q and using the fact that tensor distributes w.r.t. coproducts, we get

$$(P^* \otimes_A Q) \oplus (P_1^* \otimes_A Q) \cong (P^* \oplus P_1^*) \otimes_A Q \cong F^* \otimes_A Q.$$

Now, the proof of Proposition 33.17 goes through because F is free and finitely generated, so

$$\alpha_\otimes \colon (P^* \otimes_A Q) \oplus (P_1^* \otimes_A Q) \cong F^* \otimes_A Q \longrightarrow \mathrm{Hom}_A(F, Q) \cong \mathrm{Hom}_A(P, Q) \oplus \mathrm{Hom}_A(P_1, Q)$$

is an isomorphism and as $\alpha_\otimes$ maps $P^* \otimes_A Q$ to $\mathrm{Hom}_A(P, Q)$, it yields an isomorphism between these two spaces. □

The isomorphism $\alpha_\otimes \colon P^* \otimes_A Q \cong \mathrm{Hom}_A(P, Q)$ of Proposition 35.11 is still given by

$$\alpha_\otimes(u^* \otimes f)(x) = u^*(x)f, \qquad u^* \in P^*,\ f \in Q,\ x \in P.$$

It is convenient to introduce the *evaluation map*, $\mathrm{Ev}_x \colon P^* \otimes_A Q \to Q$, defined for every $x \in P$ by

$$\mathrm{Ev}_x(u^* \otimes f) = u^*(x)f, \qquad u^* \in P^*,\ f \in Q.$$

We will need the following generalization of part (4) of Proposition 33.13.

Proposition 35.12. *Given any two families of A-modules $(M_i)_{i\in I}$ and $(N_j)_{j\in J}$ (where I and J are finite index sets), we have an isomorphism*

$$\Big(\bigoplus_{i\in I} M_i\Big) \otimes \Big(\bigoplus_{j\in I} M_j\Big) \approx \bigoplus_{(i,j)\in I\times J} (M_i \otimes N_j).$$

Proposition 35.12 also holds for infinite index sets.

Proposition 35.13. *Let M and N be two A-module with N a free module, and pick any basis $(v_1, \ldots, v_n)$ for N. Then, every element of $M \otimes N$ can expressed in a unique way as a sum of the form*

$$u_1 \otimes v_1 + \cdots + u_n \otimes v_n, \quad u_i \in M,$$

so that $M \otimes N$ is isomorphic to M^n (as an A-module).

Proof. Since N is free with basis $(v_1, \ldots, v_n)$, we have an isomorphism

$$N \approx Av_1 \oplus \cdots \oplus Av_n.$$

By Proposition 35.12, we obtain an isomorphism

$$M \otimes N \approx M \otimes (Av_1 \oplus \cdots \oplus Av_n) \approx (M \otimes Av_1) \oplus \cdots \oplus (M \otimes Av_n).$$

Because $(v_1, \ldots, v_n)$ is a basis of N, each v_j is torsion-free so the map $a \mapsto av_j$ is an isomorphism of A onto Av_j, and because $M \otimes A \approx M$, we have the isomorphism

$$M \otimes N \approx (M \otimes A) \oplus \cdots \oplus (M \otimes A) \approx M \oplus \cdots \oplus M = M^n,$$

as claimed. □

Proposition 35.13 also holds for an infinite basis $(v_j)_{j \in J}$ of N. Obviously, a version of Proposition 35.13 also holds if M is free and N is arbitrary.

The next proposition will be also be needed.

Proposition 35.14. *Given any A-module M and any ideal $\mathfrak{a}$ in A, there is an isomorphism*

$$(A/\mathfrak{a}) \otimes_A M \approx M/\mathfrak{a}M$$

given by the map $(\overline{a} \otimes u) \mapsto au \pmod{\mathfrak{a}M}$, for all $\overline{a} \in A/\mathfrak{a}$ and all $u \in M$.

Sketch of proof. Consider the map $\varphi \colon (A/\mathfrak{a}) \times M \to M/\mathfrak{a}M$ given by

$$\varphi(\overline{a}, u) = au \pmod{\mathfrak{a}M}$$

for all $\overline{a} \in A/\mathfrak{a}$ and all $u \in M$. It is immediately checked that φ is well-defined because $au \pmod{\mathfrak{a}M}$ does not depend on the representative $a \in A$ chosen in the equivalence class $\overline{a}$, and φ is bilinear. Therefore, φ induces a linear map $\varphi \colon (A/\mathfrak{a}) \otimes M \to M/\mathfrak{a}M$, such that $\varphi(\overline{a} \otimes u) = au \pmod{\mathfrak{a}M}$. We also define the map $\psi \colon M \to (A/\mathfrak{a}) \otimes M$ by

$$\psi(u) = \overline{1} \otimes u.$$

Since $\mathfrak{a}M$ is generated by vectors of the form au with $a \in \mathfrak{a}$ and $u \in M$, and since

$$\psi(au) = \overline{1} \otimes au = \overline{a} \otimes u = 0 \otimes u = 0,$$

we see that $\mathfrak{a}M \subseteq \mathrm{Ker}\,(\psi)$, so ψ induces a linear map $\psi \colon M/\mathfrak{a}M \to (A/\mathfrak{a}) \otimes M$. We have

$$\begin{aligned} \psi(\varphi(\overline{a} \otimes u)) &= \psi(au) \\ &= \overline{1} \otimes au \\ &= \overline{a} \otimes u \end{aligned}$$

and

$$\begin{aligned}\varphi(\psi(u)) &= \varphi(\overline{1}\otimes u)\\ &= 1u\\ &= u,\end{aligned}$$

which shows that φ and ψ are mutual inverses. □

We now develop the theory necessary to understand the structure of finitely generated modules over a PID.

35.4 Torsion Modules over a PID; The Primary Decomposition

We begin by considering modules over a product ring obtained from a direct decomposition, as in Definition 32.3. In this section and the next, we closely follow Bourbaki [26] (Chapter VII). Let A be a commutative ring and let $(\mathfrak{b}_1, \ldots, \mathfrak{b}_n)$ be ideals in A such that there is an isomorphism $A \approx A/\mathfrak{b}_1 \times \cdots \times A/\mathfrak{b}_n$. From Theorem 32.16 part (b), there exist some elements $e_1, \ldots, e_n$ of A such that

$$\begin{aligned}e_i^2 &= e_i\\ e_ie_j &= 0, \quad i \neq j\\ e_1 + \cdots + e_n &= 1_A,\end{aligned}$$

and $\mathfrak{b}_i = (1_A - e_i)A$, for $i, j = 1, \ldots, n$.

Given an A-module M with $A \approx A/\mathfrak{b}_1 \times \cdots \times A/\mathfrak{b}_n$, let M_i be the subset of M annihilated by $\mathfrak{b}_i$; that is,

$$M_i = \{x \in M \mid bx = 0, \text{ for all } b \in \mathfrak{b}_i\}.$$

Because $\mathfrak{b}_i$ is an ideal, each M_i is a submodule of M. Observe that if $\lambda, \mu \in A$, $b \in \mathfrak{b}_i$, and if $\lambda - \mu = b$, then for any $x \in M_i$, since $bx = 0$,

$$\lambda x = (\mu + b)x = \mu x + bx = \mu x,$$

so M_i can be viewed as a $A/\mathfrak{b}_i$- module.

Proposition 35.15. *Given a ring $A \approx A/\mathfrak{b}_1 \times \cdots \times A/\mathfrak{b}_n$ as above, the A-module M is the direct sum*

$$M = M_1 \oplus \cdots \oplus M_n,$$

where M_i is the submodule of M annihilated by $\mathfrak{b}_i$.

Proof. For $i = 1, \dots, n$, let $p_i \colon M \to M$ be the map given by

$$p_i(x) = e_i x, \quad x \in M.$$

The map p_i is clearly linear, and because of the properties satisfied by the e_is, we have

$$\begin{aligned} p_i^2 &= p_i \\ p_i p_j &= 0, \quad i \neq j \\ p_1 + \cdots + p_n &= \mathrm{id}. \end{aligned}$$

This shows that the p_i are projections, and by Proposition 6.8 (which also holds for modules), we have a direct sum

$$M = p_1(M) \oplus \cdots \oplus p_n(M) = e_1 M \oplus \cdots \oplus e_n M.$$

It remains to show that $M_i = e_i M$. Since $(1 - e_i)e_i = e_i - e_i^2 = e_i - e_i = 0$, we see that $e_i M$ is annihilated by $\mathfrak{b}_i = (1 - e_i)A$. Furthermore, for $i \neq j$, for any $x \in M$, we have $(1 - e_i)e_j x = (e_j - e_i e_j)x = e_j x$, so no nonzero element of $e_j M$ is annihilated by $1 - e_i$, and thus not annihilated by $\mathfrak{b}_i$. It follows that $e_i M = M_i$, as claimed. □

Definition 35.8. Given an A-module M, for any nonzero $\alpha \in A$, let

$$M(\alpha) = \{x \in M \mid \alpha x = 0\},$$

the submodule of M annihilated by α. If α divides β, then $M(\alpha) \subseteq M(\beta)$, so we can define

$$M_\alpha = \bigcup_{n \geq 1} M(\alpha^n) = \{x \in M \mid (\exists n \geq 1)(\alpha^n x = 0)\},$$

the submodule of M consisting of all elements of M annihilated by some power of α.

If N is any submodule of M, it is clear that

$$N_\alpha = M \cap M_\alpha.$$

Recall that in a PID, an irreducible element is also called a *prime element*.

Definition 35.9. If A is a PID and p is a prime element in A, we say that a module M is *p-primary* if $M = M_p$.

Proposition 35.16. *Let M be module over a PID A. For every nonzero $\alpha \in A$, if*

$$\alpha = u p_1^{n_1} \cdots p_r^{n_r}$$

is a factorization of α into prime factors (where u is a unit), then the module $M(\alpha)$ annihilated by α is the direct sum

$$M(\alpha) = M(p_1^{n_1}) \oplus \cdots \oplus M(p_r^{n_r}).$$

Furthermore, the projection from $M(\alpha)$ onto $M(p_i^{n_i})$ is of the form $x \mapsto \gamma_i x$, for some $\gamma_i \in A$, and

$$M(p_i^{n_i}) = M(\alpha) \cap M_{p_i}.$$

Proof. First observe that since $M(\alpha)$ is annihilated by α, we can view $M(\alpha)$ as a $A/(\alpha)$-module. By the Chinese remainder theorem (Theorem 32.15) applied to the ideals $(up_1^{n_1}) = (p_1^{n_1}), (p_2^{n_2}), \ldots, (p_r^{n_r})$, we have an isomorphism

$$A/(\alpha) \approx A/(p_1^{n_1}) \times \cdots \times A/(p_r^{n_r}).$$

Since we also have isomorphisms

$$A/(p_i^{n_i}) \approx (A/(\alpha))/((p_i^{n_i})/(\alpha)),$$

we can apply Proposition 35.15, and we get a direct sum

$$M(\alpha) = N_1 \oplus \cdots \oplus N_r,$$

where N_i is the $A/(\alpha)$-submodule of $M(\alpha)$ annihilated by $(p_i^{n_i})/(\alpha)$, and the projections onto the N_i are of the form stated in the proposition. However, N_i is just the A-module $M(p_i^{n_i})$ annihilated by $p_i^{n_i}$, because every nonzero element of $(p_i^{n_i})/(\alpha)$ is an equivalence class modulo (α) of the form $\overline{ap_i^{n_i}}$ for some nonzero $a \in A$, and by definition, $x \in N_i$ iff

$$0 = \overline{ap_i^{n_i}}\, x = ap_i^{n_i} x, \quad \text{for all } a \in A - \{0\},$$

in particular for $a = 1$, which implies that $x \in M(p_i^{n_i})$.

The inclusion $M(p_i^{n_i}) \subseteq M(\alpha) \cap M_{p_i}$ is clear. Conversely, pick $x \in M(\alpha) \cap M_{p_i}$, which means that $\alpha x = 0$ and $p_i^s x = 0$ for some $s \geq 1$. If $s < n_i$, we are done, so assume $s \geq n_i$. Since $p_i^{n_i}$ is a gcd of α and p_i^s, by Bezout, we can write

$$p_i^{n_i} = \lambda p_i^s + \mu\alpha$$

for some $\lambda, \mu \in A$, and then $p_i^{n_i} x = \lambda p_i^s x + \mu\alpha x = 0$, which shows that $x \in M(p_i^{n_i})$, as desired. □

Here is an example of Proposition 35.16. Let $M = \mathbb{Z}/60\mathbb{Z}$, where M is considered as a $\mathbb{Z}$-module. A element in M is denoted by $\overline{x}$, where x is an integer with $0 \leq x \leq 59$. Let $\alpha = 6$ and define

$$M(6) = \{\overline{x} \in M \mid 6\overline{x} = \overline{0}\} = \{\overline{0}, \overline{10}, \overline{20}, \overline{30}, \overline{40}, \overline{50}\}.$$

Since $6 = 2 \cdot 3$, Proposition 35.16 implies that $M(6) = M(2) \oplus M(3)$, where

$$\begin{aligned} M(2) &= \{\overline{x} \in M \mid 2\overline{x} = \overline{0}\} = \{\overline{0}, \overline{30}\} \\ M(3) &= \{\overline{x} \in M \mid 3\overline{x} = \overline{0}\} = \{\overline{0}, \overline{20}, \overline{40}\}. \end{aligned}$$

Recall that if M is a torsion module over a ring A which is an integral domain, then every finite set of elements $x_1, \ldots, x_n$ in M is annihilated by $a = a_1 \cdots a_n$, where each a_i annihilates x_i.

Since A is a PID, we can pick a set P of irreducible elements of A such that every nonzero nonunit of A has a unique factorization up to a unit. Then, we have the following structure theorem for torsion modules which holds even for modules that are not finitely generated.

Theorem 35.17. *(Primary Decomposition Theorem) Let M be a torsion-module over a PID. For every irreducible element $p \in P$, let M_p be the submodule of M annihilated by some power of p. Then, M is the (possibly infinite) direct sum*

$$M = \bigoplus_{p \in P} M_p.$$

Proof. Since M is a torsion-module, for every $x \in M$, there is some $\alpha \in A$ such that $x \in M(\alpha)$. By Proposition 35.16, if $\alpha = up_1^{n_1} \cdots p_r^{n_r}$ is a factorization of α into prime factors (where u is a unit), then the module $M(\alpha)$ is the direct sum

$$M(\alpha) = M(p_1^{n_1}) \oplus \cdots \oplus M(p_r^{n_r}).$$

This means that x can be written as

$$x = \sum_{p \in P} x_p, \quad x_p \in M_p,$$

with only finitely many x_p nonzero. If

$$\sum_{p \in P} x_p = \sum_{p \in P} y_p$$

for all $p \in P$, with only finitely many x_p and y_p nonzero, then x_p and y_p are annihilated by some common nonzero element $a \in A$, so $x_p, y_p \in M(a)$. By Proposition 35.16, we must have $x_p = y_p$ for all p, which proves that we have a direct sum. □

It is clear that if p and p' are two irreducible elements such that $p = up'$ for some unit u, then $M_p = M_{p'}$. Therefore, M_p only depends on the ideal (p).

Definition 35.10. Given a torsion-module M over a PID, the modules M_p associated with irreducible elements in P are called the *p-primary components* of M.

The p-primary components of a torsion module uniquely determine the module, as shown by the next proposition.

Proposition 35.18. *Two torsion modules M and N over a PID are isomorphic iff for every every irreducible element $p \in P$, the p-primary components M_p and N_p of M and N are isomorphic.*

Proof. Let $f \colon M \to N$ be an isomorphism. For any $p \in P$, we have $x \in M_p$ iff $p^k x = 0$ for some $k \geq 1$, so

$$0 = f(p^k x) = p^k f(x),$$

which shows that $f(x) \in N_p$. Therefore, f restricts to a linear map $f \mid M_p$ from M_p to N_p. Since f is an isomorphism, we also have a linear map $f^{-1} \colon M \to N$, and our previous reasoning shows that f^{-1} restricts to a linear map $f^{-1} \mid N_p$ from N_p to M_p. But, $f \mid M_p$ and $f^{-1} \mid N_p$ are mutual inverses, so M_p and N_p are isomorphic.

Conversely, if $M_p \approx N_p$ for all $p \in P$, by Theorem 35.17, we get an isomorphism between $M = \bigoplus_{p\in P} M_p$ and $N = \bigoplus_{p\in P} N_p$. □

In view of Proposition 35.18, the direct sum of Theorem 35.17 in terms of its p-primary components is called the *canonical primary decomposition* of M.

If M is a finitely generated torsion-module, then Theorem 35.17 takes the following form.

Theorem 35.19. *(Primary Decomposition Theorem for finitely generated torsion modules) Let M be a finitely generated torsion-module over a PID A. If $\mathrm{Ann}(M) = (a)$ and if $a = up_1^{n_1} \cdots p_r^{n_r}$ is a factorization of a into prime factors, then M is the finite direct sum*

$$M = \bigoplus_{i=1}^{r} M(p_i^{n_i}).$$

Furthermore, the projection of M over $M(p_i^{n_i})$ is of the form $x \mapsto \gamma_i x$, for some $\gamma_i \in A$.

Proof. This is an immediate consequence of Proposition 35.16. □

Theorem 35.19 applies when $A = \mathbb{Z}$. In this case, M is a finitely generated torsion abelian group, and the theorem says that such a group is the direct sum of a finite number of groups whose elements have order some power of a prime number p. In particular, consider the $\mathbb{Z}$-module $\mathbb{Z}/10\mathbb{Z}$ where

$$\mathbb{Z}/10\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}\}.$$

Clearly $\mathbb{Z}/10\mathbb{Z}$ is generated by $\overline{1}$ and $\mathrm{Ann}\,(\mathbb{Z}/10\mathbb{Z}) = 10$. Theorem 35.19 implies that

$$\mathbb{Z}/10\mathbb{Z} = M(2) \oplus M(5),$$

where

$$\begin{aligned} M(2) &= \{\overline{x} \in M \mid 2\overline{x} = \overline{0}\} = \{\overline{0}, \overline{5}\} \\ M(5) &= \{\overline{x} \in M \mid 5\overline{x} = \overline{0}\} = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\}. \end{aligned}$$

Theorem 35.17 has several useful corollaries.

Proposition 35.20. *If M is a torsion module over a PID, for every submodule N of M, we have a direct sum*

$$N = \bigoplus_{p\in P} N \cap M_p.$$

Proof. It is easily verified that $N \cap M_p$ is the p-primary component of N. □

Proposition 35.21. *If M is a torsion module over a PID, a submodule N of M is a direct factor of M iff N_p is a direct factor of M_p for every irreducible element $p \in A$.*

Proof. This is because if N and N' are two submodules of M, we have $M = N \oplus N'$ iff, by Proposition 35.20, $M_p = N_p \oplus N'_p$ for every irreducible elements $p \in A$. □

Definition 35.11. An A-module M is said to be *semi-simple* iff for every submodule N of M, there is some submodule N' of M such that $M = N \oplus N'$.

Proposition 35.22. *Let A be a PID which is not a field, and let M be any A-module. Then M is semi-simple iff it is a torsion module and if $M_p = M(p)$ for every irreducible element $p \in A$ (in other words, if $x \in M$ is annihilated by a power of p, then it is already annihilated by p).*

Proof. Assume that M is semi-simple. Let $x \in M$ and pick any irreducible element $p \in A$. Then, the submodule pAx has a supplement N such that

$$M = pAx \oplus N,$$

so we can write $x = pax + y$, for some $y \in N$ and some $a \in A$. But then,

$$y = (1 - pa)x,$$

and since p is irreducible, p is not a unit, so $1 - pa \neq 0$. Observe that

$$p(1 - ap)x = py \in pAx \cap N = (0).$$

Since $p(1 - ap) \neq 0$, x is a torsion element, and thus M is a torsion module. The above argument shows that

$$p(1 - ap)x = 0,$$

which implies that $px = ap^2x$, and by induction,

$$px = a^n p^{n+1} x, \quad \text{for all } n \geq 1.$$

If we pick x in M_p, then there is some $m \geq 1$ such that $p^m x = 0$, and we conclude that

$$px = 0.$$

Therefore, $M_p = M(p)$, as claimed.

Conversely, assume that M is a torsion-module and that $M_p = M(p)$ for every irreducible element $p \in A$. By Proposition 35.21, it is sufficient to prove that a module annihilated by a an irreducible element is semi-simple. This is because such a module is a vector space over the field $A/(p)$ (recall that in a PID, an ideal (p) is maximal iff p is irreducible), and in a vector space, every subspace has a supplement. □

Theorem 35.19 shows that a finitely generated torsion module is a direct sum of p-primary modules M_p. We can do better. In the next section we show that each primary module M_p is the direct sum of cyclic modules of the form $A/(p^n)$.

35.5 Finitely Generated Modules over a PID; Invariant Factor Decomposition

There are several ways of obtaining the decomposition of a finitely generated module as a direct sum of cyclic modules. One way to proceed is to first use the Primary Decomposition Theorem and then to show how each primary module M_p is the direct sum of cyclic modules of the form $A/(p^n)$. This is the approach followed by Lang [108] (Chapter III, section 7), among others. We prefer to use a proposition that produces a particular basis for a submodule of a finitely generated free module, because it yields more information. This is the approach followed in Dummitt and Foote [55] (Chapter 12) and Bourbaki [26] (Chapter VII). The proof that we present is due to Pierre Samuel.

Proposition 35.23. *Let F be a finitely generated free module over a PID A, and let M be any submodule of F. Then, M is a free module and there is a basis $(e_1, ..., e_n)$ of F, some $q \leq n$, and some nonzero elements $a_1, \ldots, a_q \in A$, such that $(a_1e_1, \ldots, a_qe_q)$ is a basis of M and a_i divides a_{i+1} for all i, with $1 \leq i \leq q-1$.*

Proof. The proposition is trivial when $M = \{0\}$, thus assume that M is nontrivial. Pick some basis $(u_1, \ldots, u_n)$ for F. Let $L(F, A)$ be the set of linear forms on F. For any $f \in L(F, A)$, it is immediately verified that $f(M)$ is an ideal in A. Thus, $f(M) = a_hA$, for some $a_h \in A$, since every ideal in A is a principal ideal. Since A is a PID, any nonempty family of ideals in A has a maximal element, so let f be a linear map such that a_hA is a maximal ideal in A. Let $\pi_i \colon F \to A$ be the i-th projection, i.e., π_i is defined such that $\pi_i(x_1u_1 + \cdots + x_nu_n) = x_i$. It is clear that π_i is a linear map, and since M is nontrivial, one of the $\pi_i(M)$ is nontrivial, and $a_h \neq 0$. There is some $e' \in M$ such that $f(e') = a_h$.

We claim that, for every $g \in L(F, A)$, the element $a_h \in A$ divides $g(e')$.

Indeed, if d is the gcd of a_h and $g(e')$, by the Bézout identity, we can write

$$d = ra_h + sg(e'),$$

for some $r, s \in A$, and thus

$$d = rf(e') + sg(e') = (rf + sg)(e').$$

However, $rf + sg \in L(F, A)$, and thus,

$$a_hA \subseteq dA \subseteq (rf + sg)(M),$$

since d divides a_h, and by maximality of a_hA, we must have $a_hA = dA$, which implies that $d = a_h$, and thus, a_h divides $g(e')$. In particular, a_h divides each $\pi_i(e')$ and let $\pi_i(e') = a_hb_i$, with $b_i \in A$.

Let $e = b_1u_1 + \cdots + b_nu_n$. Note that

$$e' = \pi_1(e')u_1 + \cdots + \pi_n(e')u_n = a_hb_1u_1 + \cdots + a_hb_nu_n,$$

and thus, $e' = a_h e$. Since $a_h = f(e') = f(a_h e) = a_h f(e)$, and since $a_h \neq 0$, we must have $f(e) = 1$.

Next, we claim that

$$F = Ae \oplus f^{-1}(0)$$

and

$$M = Ae' \oplus (M \cap f^{-1}(0)),$$

with $e' = a_h e$.

Indeed, every $x \in F$ can be written as

$$x = f(x)e + (x - f(x)e),$$

and since $f(e) = 1$, we have $f(x - f(x)e) = f(x) - f(x)f(e) = f(x) - f(x) = 0$. Thus, $F = Ae + f^{-1}(0)$. Similarly, for any $x \in M$, we have $f(x) = ra_h$, for some $r \in A$, and thus,

$$x = f(x)e + (x - f(x)e) = ra_h e + (x - f(x)e) = re' + (x - f(x)e),$$

we still have $x - f(x)e \in f^{-1}(0)$, and clearly, $x - f(x)e = x - ra_h e = x - re' \in M$, since $e' \in M$. Thus, $M = Ae' + (M \cap f^{-1}(0))$.

To prove that we have a direct sum, it is enough to prove that $Ae \cap f^{-1}(0) = \{0\}$. For any $x = re \in Ae$, if $f(x) = 0$, then $f(re) = rf(e) = r = 0$, since $f(e) = 1$ and, thus, $x = 0$. Therefore, the sums are direct sums.

We can now prove that M is a free module by induction on the size, q, of a maximal linearly independent family for M.

If $q = 0$, the result is trivial. Otherwise, since

$$M = Ae' \oplus (M \cap f^{-1}(0)),$$

it is clear that $M \cap f^{-1}(0)$ is a submodule of F and that every maximal linearly independent family in $M \cap f^{-1}(0)$ has at most $q - 1$ elements. By the induction hypothesis, $M \cap f^{-1}(0)$ is a free module, and by adding e' to a basis of $M \cap f^{-1}(0)$, we obtain a basis for M, since the sum is direct.

The second part is shown by induction on the dimension n of F.

The case $n = 0$ is trivial. Otherwise, since

$$F = Ae \oplus f^{-1}(0),$$

and since, by the previous argument, $f^{-1}(0)$ is also free, $f^{-1}(0)$ has dimension $n - 1$. By the induction hypothesis applied to its submodule $M \cap f^{-1}(0)$, there is a basis $(e_2, \ldots, e_n)$ of $f^{-1}(0)$, some $q \leq n$, and some nonzero elements $a_2, \ldots, a_q \in A$, such that, $(a_2 e_2, \ldots, a_q e_q)$ is a basis of $M \cap f^{-1}(0)$, and a_i divides a_{i+1} for all i, with $2 \leq i \leq q - 1$. Let $e_1 = e$, and $a_1 = a_h$, as above. It is clear that $(e_1, \ldots, e_n)$ is a basis of F, and that that $(a_1 e_1, \ldots, a_q e_q)$

is a basis of M, since the sums are direct, and $e' = a_1 e_1 = a_h e$. It remains to show that a_1 divides a_2. Consider the linear map $g\colon F \to A$ such that $g(e_1) = g(e_2) = 1$, and $g(e_i) = 0$, for all i, with $3 \leq i \leq n$. We have $a_h = a_1 = g(a_1 e_1) = g(e') \in g(M)$, and thus $a_h A \subseteq g(M)$. Since $a_h A$ is maximal, we must have $g(M) = a_h A = a_1 A$. Since $a_2 = g(a_2 e_2) \in g(M)$, we have $a_2 \in a_1 A$, which shows that a_1 divides a_2. □

We need the following basic proposition.

Proposition 35.24. *For any commutative ring A, if F is a free A-module and if $(e_1, \ldots, e_n)$ is a basis of F, for any elements $a_1, \ldots, a_n \in A$, there is an isomorphism*

$$F/(Aa_1e_1 \oplus \cdots \oplus Aa_ne_n) \approx (A/a_1A) \oplus \cdots \oplus (A/a_nA).$$

Proof. Let $\sigma\colon F \to A/(a_1A) \oplus \cdots \oplus A/(a_nA)$ be the linear map given by

$$\sigma(x_1e_1 + \cdots + x_ne_n) = (\overline{x}_1, \ldots, \overline{x}_n),$$

where $\overline{x}_i$ is the equivalence class of x_i in A/a_iA. The map σ is clearly surjective, and its kernel consists of all vectors $x_1e_1 + \cdots + x_ne_n$ such that $x_i \in a_iA$, for $i = 1, \ldots, n$, which means that

$$\mathrm{Ker}\,(\sigma) = Aa_1e_1 \oplus \cdots \oplus Aa_ne_n.$$

Since $M/\mathrm{Ker}\,(\sigma)$ is isomorphic to $\mathrm{Im}(\sigma)$, we get the desired isomorphism. □

We can now prove the existence part of the structure theorem for finitely generated modules over a PID.

Theorem 35.25. *Let M be a finitely generated nontrivial A-module, where A a PID. Then, M is isomorphic to a direct sum of cyclic modules*

$$M \approx A/\mathfrak{a}_1 \oplus \cdots \oplus A/\mathfrak{a}_m,$$

where the $\mathfrak{a}_i$ are proper ideals of A (possibly zero) such that

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_m \neq A.$$

More precisely, if $\mathfrak{a}_1 = \cdots = \mathfrak{a}_r = (0)$ and $(0) \neq \mathfrak{a}_{r+1} \subseteq \cdots \subseteq \mathfrak{a}_m \neq A$, then

$$M \approx A^r \oplus (A/\mathfrak{a}_{r+1} \oplus \cdots \oplus A/\mathfrak{a}_m),$$

where $A/\mathfrak{a}_{r+1} \oplus \cdots \oplus A/\mathfrak{a}_m$ is the torsion submodule of M. The module M is free iff $r = m$, and a torsion-module iff $r = 0$. In the latter case, the annihilator of M is $\mathfrak{a}_1$.

Proof. Since M is finitely generated and nontrivial, there is a surjective homomorphism $\varphi\colon A^n \to M$ for some $n \geq 1$, and M is isomorphic to $A^n/\mathrm{Ker}\,(\varphi)$. Since $\mathrm{Ker}\,(\varphi)$ is a submodule of the free module A^n, by Proposition 35.23, $\mathrm{Ker}\,(\varphi)$ is a free module and there is a basis $(e_1, \ldots, e_n)$ of A^n and some nonzero elements $a_1, \ldots, a_q$ $(q \leq n)$ such that $(a_1e_1, \ldots, a_qe_q)$ is a basis of $\mathrm{Ker}\,(\varphi)$ and $a_1 \mid a_2 \mid \cdots \mid a_q$. Let $a_{q+1} = \ldots = a_n = 0$.

By Proposition 35.24, we have an isomorphism

$$A^n/\mathrm{Ker}\,(\varphi) \approx A/a_1A \oplus \cdots \oplus A/a_nA.$$

Whenever a_i is unit, the factor $A/a_iA = (0)$, so we can weed out the units. Let $r = n - q$, and let $s \in \mathbb{N}$ be the smallest index such that a_{s+1} is not a unit. Note that $s = 0$ means that there are no units. Also, as $M \neq (0)$, $s < n$. Then,

$$M \approx A^n/\mathrm{Ker}\,(\varphi) \approx A/a_{s+1}A \oplus \cdots \oplus A/a_nA.$$

Let $m = r + q - s = n - s$. Then, we have the sequence

$$\underbrace{a_{s+1}, \ldots, a_q}_{q-s}, \underbrace{a_{q+1}, \ldots, a_n}_{r=n-q},$$

where $a_{s+1} \mid a_{s+2} \mid \cdots \mid a_q$ are nonzero and nonunits and $a_{q+1} = \cdots = a_n = 0$, so we define the m ideals $\mathfrak{a}_i$ as follows:

$$\mathfrak{a}_i = \begin{cases} (0) & \text{if } 1 \leq i \leq r \\ a_{r+q+1-i}A & \text{if } r+1 \leq i \leq m. \end{cases}$$

With these definitions, the ideals $\mathfrak{a}_i$ are proper ideals and we have

$$\mathfrak{a}_i \subseteq \mathfrak{a}_{i+1}, \quad i = 1, \ldots, m-1.$$

When $r = 0$, since $a_{s+1} \mid a_{s+2} \mid \cdots \mid a_n$, it is clear that $\mathfrak{a}_1 = a_nA$ is the annihilator of M. The other statements of the theorem are clear. □

Example 35.1. Here is an example of Theorem 35.25. Let M be a $\mathbb{Z}$-module with generators $\{e_1, e_2, e_3, e_4\}$ subject to the relations $6e_3 = 0$, $2e_4 = 0$. Then

$$M \cong \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z},$$

where

$$\mathfrak{a}_1 = (0), \qquad \mathfrak{a}_2 = (0), \qquad \mathfrak{a}_3 = (6), \qquad \mathfrak{a}_4 = (2).$$

The natural number r is called the *free rank* or *Betti number* of the module M. The generators $\alpha_1, \ldots, \alpha_m$ of the ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$ (defined up to a unit) are often called the *invariant factors* of M (in the notation of Theorem 35.25, the generators of the ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$ are denoted by $a_q, \ldots, a_{s+1}$, $s \leq q$).

As corollaries of Theorem 35.25, we obtain again the following facts established in Section 35.1:

1. A finitely generated module over a PID is the direct sum of its torsion module and a free module.

2. A finitely generated torsion-free module over a PID is free.

It turns out that the ideals $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_m \neq A$ are uniquely determined by the module M. Uniqueness proofs found in most books tend to be intricate and not very intuitive. The shortest proof that we are aware of is from Bourbaki [26] (Chapter VII, Section 4), and uses wedge products.

The following preliminary results are needed.

Proposition 35.26. *If A is a commutative ring and if $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$ are ideals of A, then there is an isomorphism*

$$A/\mathfrak{a}_1 \otimes \cdots \otimes A/\mathfrak{a}_m \approx A/(\mathfrak{a}_1 + \cdots + \mathfrak{a}_m).$$

Sketch of proof. We proceed by induction on m. For $m = 2$, we define the map $\varphi\colon A/\mathfrak{a}_1 \times A/\mathfrak{a}_2 \to A/(\mathfrak{a}_1 + \mathfrak{a}_2)$ by

$$\varphi(\overline{a}, \overline{b}) = ab \pmod{\mathfrak{a}_1 + \mathfrak{a}_2}.$$

It is well-defined because if $a' = a + a_1$ and $b' = b + a_2$ with $a_1 \in \mathfrak{a}_1$ and $a_2 \in \mathfrak{a}_2$, then

$$a'b' = (a + a_1)(b + a_2) = ab + ba_1 + aa_2 + a_1a_2,$$

and so

$$a'b' \equiv ab \pmod{\mathfrak{a}_1 + \mathfrak{a}_2}.$$

It is also clear that this map is bilinear, so it induces a linear map $\varphi\colon A/\mathfrak{a}_1 \otimes A/\mathfrak{a}_2 \to A/(\mathfrak{a}_1 + \mathfrak{a}_2)$ such that $\varphi(\overline{a} \otimes \overline{b}) = ab \pmod{\mathfrak{a}_1 + \mathfrak{a}_2}$.

Next, observe that any arbitrary tensor

$$\overline{a}_1 \otimes \overline{b}_1 + \cdots + \overline{a}_n \otimes \overline{b}_n$$

in $A/\mathfrak{a}_1 \otimes A/\mathfrak{a}_2$ can be rewritten as

$$\overline{1} \otimes (\overline{a_1b_1} + \cdots + \overline{a_nb_n}),$$

which is of the form $\overline{1} \otimes \overline{s}$, with $s \in A$. We can use this fact to show that φ is injective and surjective, and thus an isomorphism.

For example, if $\varphi(\overline{1} \otimes \overline{s}) = 0$, because $\varphi(\overline{1} \otimes \overline{s}) = s \pmod{\mathfrak{a}_1 + \mathfrak{a}_2}$, we have $s \in \mathfrak{a}_1 + \mathfrak{a}_2$, so we can write $s = a + b$ with $a \in \mathfrak{a}_1$ and $b \in \mathfrak{a}_2$. Then

$$\begin{aligned}\overline{1} \otimes \overline{s} &= \overline{1} \otimes \overline{a+b} \\ &= \overline{1} \otimes (\overline{a} + \overline{b}) \\ &= \overline{1} \otimes \overline{a} + \overline{1} \otimes \overline{b} \\ &= \overline{a} \otimes \overline{1} + \overline{1} \otimes \overline{b} \\ &= 0 + 0 = 0,\end{aligned}$$

since $a \in \mathfrak{a}_1$ and $b \in \mathfrak{a}_2$, which proves injectivity. □

Recall that the exterior algebra of an A-module M is defined by

$$\bigwedge M = \bigoplus_{k \geq 0} \bigwedge^k (M).$$

Proposition 35.27. *If A is a commutative ring, then for any n modules M_i, there is an isomorphism*

$$\bigwedge (\bigoplus_{i=1}^n M_i) \approx \bigotimes_{i=1}^n \bigwedge M_i.$$

A proof can be found in Bourbaki [25] (Chapter III, Section 7, No 7, Proposition 10).

Proposition 35.28. *Let A be a commutative ring and let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be n ideals of A. If the module M is the direct sum of n cyclic modules*

$$M = A/\mathfrak{a}_1 \oplus \cdots \oplus A/\mathfrak{a}_n,$$

then for every $p > 0$, the exterior power $\bigwedge^p M$ is isomorphic to the direct sum of the modules $A/\mathfrak{a}_H$, where H ranges over all subsets $H \subseteq \{1, \ldots, n\}$ with p elements, and with

$$\mathfrak{a}_H = \sum_{h \in H} \mathfrak{a}_h.$$

Proof. If u_i is the image of 1 in $A/\mathfrak{a}_i$, then $A/\mathfrak{a}_i$ is equal to Au_i. By Proposition 35.27, we have

$$\bigwedge M \approx \bigotimes_{i=1}^n \bigwedge (Au_i).$$

We also have

$$\bigwedge (Au_i) = \bigoplus_{k \geq 0} \bigwedge^k (Au_i) \approx A \oplus Au_i,$$

since $au_i \wedge bu_i = 0$, and it follows that

$$\bigwedge^p M \approx \bigoplus_{\substack{H \subseteq \{1,\ldots,n\} \\ H=\{k_1,\ldots,k_p\}}} (Au_{k_1}) \otimes \cdots \otimes (Au_{k_p}).$$

However, by Proposition 35.26, we have

$$(Au_{k_1}) \otimes \cdots \otimes (Au_{k_p}) = A/\mathfrak{a}_{k_1} \otimes \cdots \otimes A/\mathfrak{a}_{k_p} \approx A/(\mathfrak{a}_{k_1} + \cdots + \mathfrak{a}_{k_p}) = A/\mathfrak{a}_H.$$

Therefore,

$$\bigwedge^p M \approx \bigoplus_{\substack{H \subseteq \{1,\ldots,n\} \\ |H|=p}} A/\mathfrak{a}_H,$$

as claimed. □

Example 35.1 continued: Recall that M is the $\mathbb{Z}$-module generated by $\{e_1, e_2, e_3, e_4\}$ subject to $6e_3 = 0$, $2e_2 = 0$. Then

$$\begin{aligned}
\bigwedge^1 M &= \mathrm{span}\{e_1, e_2, e_3, e_4\} \\
\bigwedge^2 M &= \mathrm{span}\{e_1 \wedge e_2, e_1 \wedge e_3, e_1 \wedge e_4, e_2 \wedge e_3, e_2 \wedge e_4, e_3 \wedge e_4\} \\
\bigwedge^3 M &= \mathrm{span}\{e_1 \wedge e_2 \wedge e_3, e_1 \wedge e_2 \wedge e_4, e_1 \wedge e_3 \wedge e_4, e_2 \wedge e_3 \wedge e_4\} \\
\bigwedge^3 M &= \mathrm{span}\{e_1 \wedge e_2 \wedge e_3 \wedge e_4\}.
\end{aligned}$$

Since $6e_3 = 0$, each element of $\{e_1 \wedge e_3, e_2 \wedge e_3, e_1 \wedge e_2 \wedge e_3\}$ is annihilated by $6\mathbb{Z} = (6)$. Since $2e_4 = 0$, each element of $\{e_1 \wedge e_4, e_2 \wedge e_4, e_3 \wedge e_4, e_1 \wedge e_2 \wedge e_4, e_1 \wedge e_3 \wedge e_4, e_2 \wedge e_3 \wedge e_4, e_1 \wedge e_2 \wedge e_3 \wedge e_4\}$ is annihilated by $2\mathbb{Z} = (2)$. We have shown that

$$M \cong \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}/(6) \oplus \mathbb{Z}/(2),$$

where $\mathfrak{a}_1 = (0) = \mathfrak{a}_2$, $\mathfrak{a}_3 = (6)$,and $\mathfrak{a}_4 = (2)$. Then Proposition 35.28 implies that

$$\begin{aligned}
\bigwedge^1 M &\cong \mathbb{Z}/\mathfrak{a}_1 \oplus \mathbb{Z}/\mathfrak{a}_2 \oplus \mathbb{Z}/\mathfrak{a}_3 \oplus \mathbb{Z}/\mathfrak{a}_4 = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}/(6) \oplus \mathbb{Z}/(2) \\
\bigwedge^2 M &\cong \mathbb{Z}/(\mathfrak{a}_1 + \mathfrak{a}_2) \oplus \mathbb{Z}/(\mathfrak{a}_1 + \mathfrak{a}_3) \oplus \mathbb{Z}/(\mathfrak{a}_1 + \mathfrak{a}_4) \oplus \mathbb{Z}/(\mathfrak{a}_2 + \mathfrak{a}_3) \oplus \mathbb{Z}/(\mathfrak{a}_2 + \mathfrak{a}_3) \\
&\quad \oplus \mathbb{Z}/(\mathfrak{a}_3 + \mathfrak{a}_4) = \mathbb{Z} \oplus \mathbb{Z}/(6) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(6) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \\
\bigwedge^3 M &\cong \mathbb{Z}/(\mathfrak{a}_1 + \mathfrak{a}_2 + \mathfrak{a}_3) \oplus \mathbb{Z}/(\mathfrak{a}_1 + \mathfrak{a}_2 + \mathfrak{a}_4) \oplus \mathbb{Z}/(\mathfrak{a}_1 + \mathfrak{a}_3 + \mathfrak{a}_4) \oplus \mathbb{Z}/(\mathfrak{a}_1 + \mathfrak{a}_3 + \mathfrak{a}_4) \\
&= \mathbb{Z}/(6) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}(2) \\
\bigwedge^4 M &\cong \mathbb{Z}/(\mathfrak{a}_1 + \mathfrak{a}_2 + \mathfrak{a}_3 + \mathfrak{a}_4) = \mathbb{Z}/(2).
\end{aligned}$$

When the ideals $\mathfrak{a}_i$ form a chain of inclusions $\mathfrak{a}_1 \subseteq \cdots \subseteq \mathfrak{a}_n$, we get the following remarkable result.

Proposition 35.29. *Let A be a commutative ring and let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be n ideals of A such that $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_n$. If the module M is the direct sum of n cyclic modules*

$$M = A/\mathfrak{a}_1 \oplus \cdots \oplus A/\mathfrak{a}_n,$$

then for every p with $1 \leq p \leq n$, the ideal $\mathfrak{a}_p$ is the annihilator of the exterior power $\bigwedge^p M$. If $\mathfrak{a}_n \neq A$, then $\bigwedge^p M \neq (0)$ for $p = 1, \ldots, n$, and $\bigwedge^p M = (0)$ for $p > n$.

Proof. With the notation of Proposition 35.28, we have $\mathfrak{a}_H = \mathfrak{a}_{\max(H)}$, where $\max(H)$ is the greatest element in the set H. Since $\max(H) \geq p$ for any subset with p elements and since $\max(H) = p$ when $H = \{1, \ldots, p\}$, we see that

$$\mathfrak{a}_p = \bigcap_{\substack{H \subseteq \{1,\ldots,n\} \\ |H|=p}} \mathfrak{a}_H.$$

By Proposition 35.28, we have

$$\bigwedge^p M \approx \bigoplus_{\substack{H \subseteq \{1,\ldots,n\} \\ |H|=p}} A/\mathfrak{a}_H$$

which proves that $\mathfrak{a}_p$ is indeed the annihilator of $\bigwedge^p M$. The rest is clear. □

Example 35.1 continued: Recall that M is the $\mathbb{Z}$-module generated by $\{e_1, e_2, e_3, e_4\}$ subject to $6e_3 = 0$, $2e_2 = 0$. Then

$$\begin{aligned}
\bigwedge^1 M &= \mathrm{span}\{e_1, e_2, e_3, e_4\} \\
\bigwedge^2 M &= \mathrm{span}\{e_1 \wedge e_2, e_1 \wedge e_3, e_1 \wedge e_4, e_2 \wedge e_3, e_2 \wedge e_4, e_3 \wedge e_4\} \\
\bigwedge^3 M &= \mathrm{span}\{e_1 \wedge e_2 \wedge e_3, e_1 \wedge e_2 \wedge e_4, e_1 \wedge e_3 \wedge e_4, e_2 \wedge e_3 \wedge e_4\} \\
\bigwedge^3 M &= \mathrm{span}\{e_1 \wedge e_2 \wedge e_3 \wedge e_4\}.
\end{aligned}$$

Since e_1 and e_2 are free, $e_1 \wedge e_2$ is also free. Since $6e_3 = 0$, each element of $\{e_1 \wedge e_3, e_2 \wedge e_3, e_1 \wedge e_2 \wedge e_3\}$ is annihilated by $6\mathbb{Z} = (6)$. Since $2e_4 = 0$, each element of $\{e_1 \wedge e_4, e_2 \wedge e_4, e_3 \wedge e_4, e_1 \wedge e_2 \wedge e_4, e_1 \wedge e_3 \wedge e_4, e_2 \wedge e_3 \wedge e_4, e_1 \wedge e_2 \wedge e_3 \wedge e_4\}$ is annihilated by $2\mathbb{Z} = (2)$.

Then

$$\begin{aligned}
\mathrm{Ann}(\bigwedge^{1} M) &= \mathrm{Ann}\, e_1 = (0)\\
\mathrm{Ann}(\bigwedge^{2} M) &= \mathrm{Ann}\, e_1 \wedge e_2 = (0)\\
\mathrm{Ann}(\bigwedge^{3} M) &= \mathrm{Ann}\, e_1 \wedge e_2 \wedge e_3 = (6)\\
\mathrm{Ann}(\bigwedge^{4} M) &= \mathrm{Ann}\, e_1 \wedge e_2 \wedge e_3 \wedge e_4 = (2),
\end{aligned}$$

and Proposition 35.29 provides another verification of

$$M \cong \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}/(6) \oplus \mathbb{Z}/(2).$$

Propostion 35.29 immediately implies the following crucial fact.

Proposition 35.30. *Let A be a commutative ring and let $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$ be m ideals of A and $\mathfrak{a}'_1, \ldots, \mathfrak{a}'_n$ be n ideals of A such that $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_m \neq A$ and $\mathfrak{a}'_1 \subseteq \mathfrak{a}'_2 \subseteq \cdots \subseteq \mathfrak{a}'_n \neq A$ If we have an isomorphism*

$$A/\mathfrak{a}_1 \oplus \cdots \oplus A/\mathfrak{a}_m \approx A/\mathfrak{a}'_1 \oplus \cdots \oplus A/\mathfrak{a}'_n,$$

then $m = n$ and $\mathfrak{a}_i = \mathfrak{a}'_i$ for $i = 1, \ldots, n$.

Proposition 35.30 yields the uniqueness of the decomposition in Theorem 35.25.

Theorem 35.31. *(Invariant Factors Decomposition) Let M be a finitely generated nontrivial A-module, where A a PID. Then, M is isomorphic to a direct sum of cyclic modules*

$$M \approx A/\mathfrak{a}_1 \oplus \cdots \oplus A/\mathfrak{a}_m,$$

where the $\mathfrak{a}_i$ are proper ideals of A (possibly zero) such that

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_m \neq A.$$

More precisely, if $\mathfrak{a}_1 = \cdots = \mathfrak{a}_r = (0)$ and $(0) \neq \mathfrak{a}_{r+1} \subseteq \cdots \subseteq \mathfrak{a}_m \neq A$, then

$$M \approx A^r \oplus (A/\mathfrak{a}_{r+1} \oplus \cdots \oplus A/\mathfrak{a}_m),$$

where $A/\mathfrak{a}_{r+1} \oplus \cdots \oplus A/\mathfrak{a}_m$ is the torsion submodule of M. The module M is free iff $r = m$, and a torsion-module iff $r = 0$. In the latter case, the annihilator of M is $\mathfrak{a}_1$. Furthermore, the integer r and ideals $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_m \neq A$ are uniquely determined by M.

Proof. By Theorem 35.7, since $M_{\mathrm{tor}} = A/\mathfrak{a}_{r+1} \oplus \cdots \oplus A/\mathfrak{a}_m$, we know that the dimension r of the free summand only depends on M. The uniqueness of the sequence of ideals follows from Proposition 35.30. □

In view of the uniqueness part of Theorem 35.31, we make the following definition.

Definition 35.12. Given a finitely generated module M over a PID A as in Theorem 35.31, the ideals $\mathfrak{a}_i = \alpha_i A$ are called the *invariant factors* of M. The generators α_i of these ideals (uniquely defined up to a unit) are also called the *invariant factors* of M.

Proposition 35.23 can be sharpened as follows:

Proposition 35.32. *Let F be a finitely generated free module over a PID A, and let M be any submodule of F. Then, M is a free module and there is a basis $(e_1, ..., e_n)$ of F, some $q \leq n$, and some nonzero elements $a_1, \ldots, a_q \in A$, such that $(a_1e_1, \ldots, a_qe_q)$ is a basis of M and a_i divides a_{i+1} for all i, with $1 \leq i \leq q-1$. Furthermore, the free module M' with basis $(e_1, \ldots, e_q)$ and the ideals $a_1A, \ldots, a_qA$ are uniquely determined by M; the quotient module M'/M is the torsion module of F/M, and we have an isomorphism*

$$M'/M \approx A/a_1A \oplus \cdots \oplus A/a_qA.$$

Proof. Since $a_i \neq 0$ for $i = 1, \ldots, q$, observe that

$$M' = \{x \in F \mid (\exists \beta \in A,\, \beta \neq 0)(\beta x \in M)\},$$

which shows that M'/M is the torsion module of F/M. Therefore, M' is uniquely determined. Since

$$M = Aa_1e_1 \oplus \cdots \oplus Aa_qe_q,$$

by Proposition 35.24 we have an isomorphism

$$M'/M \approx A/a_1A \oplus \cdots \oplus A/a_qA.$$

Now, it is possible that the first s elements a_i are units, in which case $A/a_iA = (0)$, so we can eliminate such factors and we get

$$M'/M \approx A/a_{s+1}A \oplus \cdots \oplus A/a_qA,$$

with $a_qA \subseteq a_{q-1}A \subseteq \cdots \subseteq a_{s+1}A \neq A$. By Proposition 35.30, $q - s$ and the ideals a_jA are uniquely determined for $j = s+1, \ldots, q$, and since $a_1A = \cdots = a_sA = A$, the q ideals a_iA are uniquely determined. □

The ideals $a_1A, \ldots, a_qA$ of Proposition 35.32 are called the *invariant factors of M with respect to F*. They *should not be confused* with the invariant factors of a module M.

It turns out that $a_1, \ldots, a_q$ can also be computed in terms of gcd's of minors of a certain matrix. Recall that if X is an $m \times n$ matrix, then a $k \times k$ minor of X is the determinant of any $k \times k$ matrix obtained by picking k columns of X, and then k rows from these k columns.

Proposition 35.33. *Let F be a free module of finite dimension over a PID, $(u_1, \ldots, u_n)$ be a basis of F, M be a submodule of F, and $(x_1, \ldots, x_m)$ be a set of generators of M. If $a_1A, \ldots, a_qA$ are the invariant factors of M with respect to F as in Proposition 35.32, then for $k = 1, \ldots, q$, the product $a_1 \cdots a_k$ is a gcd of the $k \times k$ minors of the $n \times m$ matrix X_U whose columns are the coordinates of the x_j over the u_i.*

Proof. Proposition 35.23 shows that $M \subseteq a_1F$. Consequently, the coordinates of any element of M are multiples of a_1. On the other hand, we know that there is a linear form f for which a_1A is a maximal ideal and some $e' \in M$ such that $f(e') = a_1$. If we write e' as a linear combination of the x_i, we see that a_1 belongs to the ideal spanned by the coordinates of the x_i over the basis $(u_1, \ldots, u_n)$. Since these coordinates are all multiples of a_1, it follows that a_1 is their gcd, which proves the case $k = 1$.

For any $k \geq 2$, consider the exterior power $\bigwedge^k M$. Using the notation of the proof of Proposition 35.23, the module M has the basis $(a_1e_1, \ldots, a_qe_q)$, so $\bigwedge^k M$ has a basis consisting of elements of the form

$$a_{i_1}e_{i_1} \wedge \cdots \wedge a_{i_k}e_{i_k} = a_{i_1} \cdots a_{i_k}\, e_{i_1} \wedge \cdots \wedge e_{i_k},$$

for all sequences $(i_1, \ldots, i_k)$ such that $1 \leq i_1 < i_2 < \cdots < i_k \leq q$. However, the vectors $e_{i_1} \wedge \cdots \wedge e_{i_k}$ form a basis of $\bigwedge^k F$. Thus, the map from $\bigwedge^k M$ into $\bigwedge^k F$ induced by the inclusion $M \subseteq F$ defines an isomorphism of $\bigwedge^k M$ onto the submodule of $\bigwedge^k F$ having the elements $a_{i_1} \cdots a_{i_k}\, e_{i_1} \wedge \cdots \wedge e_{i_k}$ as a basis. Since a_j is a multiple of the a_i for $i < j$, the products $a_{i_1} \cdots a_{i_k}$ are all multiples of $\delta_k = a_1 \cdots a_k$, and one of these is equal to δ_k. The reasoning used for $k = 1$ shows that δ_k is a gcd of the set of coordinates of any spanning set of $\bigwedge^k M$ over any basis of $\bigwedge^k F$. If we pick as basis of $\bigwedge^k F$ the wedge products $u_{i_1} \wedge \cdots \wedge u_{i_k}$, and as generators of $\bigwedge^k M$ the wedge products $x_{i_1} \wedge \cdots \wedge x_{i_k}$, it is easy to see that the coordinates of the $x_{i_1} \wedge \cdots \wedge x_{i_k}$ are indeed determinants which are the $k \times k$ minors of the matrix X_U. □

Proposition 35.33 yields $a_1, \ldots, a_q$ (up to units) as follows: First, a_1 is a gcd of the entries in X_U. Having computed $a_1, \ldots, a_k$, let $b_k = a_1 \cdots , a_k$, compute $b_{k+1} = a_1 \cdots a_k a_{k+1}$ as a gcd of all the $(k+1) \times (k+1)$ minors of X_U, and then a_{k+1} is obtained by dividing b_{k+1} by b_k (recall that a PID is an integral domain).

We also have the following interesting result about linear maps between free modules over a PID.

Proposition 35.34. *Let A be a PID, let F be a free module of dimension n, F' be a free module of dimension m, and $f \colon F \to F'$ be a linear map from F to F'. Then, there exist a basis $(e_1, \ldots, e_n)$ of F, a basis $(e'_1, \ldots, e'_m)$ of F', and some nonzero elements $\alpha_1, \ldots \alpha_r \in A$ such that*

$$f(e_i) = \begin{cases} \alpha_i e'_i & \textit{if } 1 \leq i \leq r \\ 0 & \textit{if } r+1 \leq i \leq n, \end{cases}$$

and $\alpha_1 \mid \alpha_2 \mid \cdots \mid \alpha_r$*. Furthermore, the ideals* $\alpha_1 A, \ldots, \alpha_r A$ *are the invariant factors of* $f(F)$ *with respect* F'*.*

Proof. Let F_0 be the kernel of f. Since $M' = f(F)$ is a submodule of the free module F', it is free, and similarly F_0 is free as a submodule of the free module F (by Proposition 35.23). By Proposition 35.2, we have

$$F = F_0 \oplus F_1,$$

where F_1 is a free module, and the restriction of f to F_1 is an isomorphism onto $M' = f(F)$. Proposition 35.32 applied to F' and M' yields a basis $(e'_1, \ldots, e'_m)$ of F' such that $(\alpha_1 e'_1, \ldots, \alpha_r e'_r)$ is a basis of M', where $\alpha_1 A, \ldots, \alpha_r A$ are the invariant factors for M' with respect to F'. Since the restriction of f to F_1 is and isomorphism, there is a basis $(e_1, \ldots, e_r)$ of F_1 such that

$$f(e_i) = \alpha_i e'_i, \quad i = 1, \ldots, r.$$

We can extend this basis to a basis of F by picking a basis of F_0 (a free module), which yields the desired result. □

The matrix version of Proposition 35.34 is the following proposition.

Proposition 35.35. *If* X *is an* $m \times n$ *matrix of rank* r *over a PID* A*, then there exist some invertible* $n \times n$ *matrix* P*, some invertible* $m \times m$ *matrix* Q*, and a* $m \times n$ *matrix* D *of the form*

$$D = \begin{pmatrix} \alpha_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \alpha_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & \alpha_r & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

for some nonzero $\alpha_i \in A$*, such that*

(1) $\alpha_1 \mid \alpha_2 \mid \cdots \mid \alpha_r$*,*

(2) $X = QDP^{-1}$*, and*

(3) The α_i*s are uniquely determined up to a unit.*

The ideals $\alpha_1 A, \ldots, \alpha_r A$ are called the *invariant factors* of the matrix X. Recall that two $m \times n$ matrices X and Y are *equivalent* iff

$$Y = QXP^{-1},$$

for some invertible matrices, P and Q. Then, Proposition 35.35 implies the following fact.

Proposition 35.36. *Two $m \times n$ matrices X and Y are equivalent iff they have the same invariant factors.*

If X is the matrix of a linear map $f\colon F \to F'$ with respect to some basis $(u_1, \ldots, u_n)$ of F and some basis $(u'_1, \ldots, u'_m)$ of F', then the columns of X are the coordinates of the $f(u_j)$ over the u'_i, where the $f(u_j)$ generate $f(F)$, so Proposition 35.33 applies and yields the following result:

Proposition 35.37. *If X is a $m \times n$ matrix or rank r over a PID A, and if $\alpha_1 A, \ldots, \alpha_r A$ are its invariant factors, then α_1 is a gcd of the entries in X, and for $k = 2, \ldots, r$, the product $\alpha_1 \cdots \alpha_k$ is a gcd of all $k \times k$ minors of X.*

There are algorithms for converting a matrix X over a PID to the form $X = QDP^{-1}$ as described in Proposition 35.35. For Euclidean domains, this can be achieved by using the elementary row and column operations $P(i,k)$, $E_{i,j;\beta}$, and $E_{i,\lambda}$ described in Chapter 8, where we require the scalar λ used in $E_{i,\lambda}$ to be a unit. For an arbitrary PID, another kind of elementary matrix (containing some 2×2 submatrix in addition to diagonal entries) is needed. These procedures involve computing gcd's and use the Bezout identity to mimic division. Such methods are presented in D. Serre [154], Jacobson [97], and Van Der Waerden [177], and sketched in Artin [7]. We describe and justify several of these methods in Section 36.5.

Proposition 35.32 has the following two applications.

First, consider a finitely presented module M over a PID given by some $m \times n$ matrix R. By Proposition 35.35, the matrix R can be diagonalized as $R = QDP^{-1}$ where D is a diagonal matrix. Then, we see that M has a presentation with m generators and r relations of the form

$$\alpha_i e_i = 0,$$

where $\alpha_i \neq 0$ and $\alpha_1 \mid \alpha_2 \mid \cdots \mid \alpha_r$.

For the second application, let F be a free module with basis $(e_1, \ldots, e_n)$, and let M be a submodule of F generated by m vectors $v_1, \ldots, v_m$ in F. The module M can be viewed as the set of linear combinations of the columns of the $n \times m$ matrix also denoted M consisting of the coordinates of the vectors $v_1, \ldots, v_m$ over the basis $(e_1, \ldots, e_n)$. Then by Proposition 35.35, the matrix R can be diagonalized as $R = QDP^{-1}$ where D is a diagonal matrix. The columns of Q form a basis $(e'_1, \ldots, e'_n)$ of F, and since $RP = QD$, the nonzero columns of RP form the basis $(a_1 e'_1, \ldots, a_q e'_q)$ of M.

When the ring A is a Euclidean domain, Theorem 36.18 shows that P and Q are products of elementary row and column operations. In particular, when $A = \mathbb{Z}$, in which cases our $\mathbb{Z}$-modules are abelian groups, we can find P and Q using Euclidean division.

If $A = \mathbb{Z}$, a finitely generated submodule M of $\mathbb{Z}^n$ is called a *lattice*. It is given as the set of integral linear combinations of a finite set of integral vectors.

Here is an example taken from Artin [7] (Chapter 12, Section 4). Let F be the free $\mathbb{Z}$-module $\mathbb{Z}^2$, and let M be the lattice generated by the columns of the matrix

$$R = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}.$$

The columns (u_1, u_2) of R are linearly independent, but they are not a basis of $\mathbb{Z}^2$. For example, in order to obtain e_1 as a linear combination of these columns, we would need to solve the linear system

$$\begin{aligned} 2x - y &= 1 \\ x + 2y &= 0. \end{aligned}$$

From the second equation, we get $x = -2y$, which yields

$$-5y = 1.$$

But, $y = -1/5$ is not an integer. We leave it as an exercise to check that

$$\begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix},$$

which means that

$$\begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix},$$

so $R = QDP^{-1}$ with

$$Q = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}, \quad P = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

The new basis (u_1', u_2') for $\mathbb{Z}^2$ consists of the columns of Q and the new basis for M consists of the columns $(u_1', 5u_2')$ of QD, where

$$QD = \begin{pmatrix} 1 & 0 \\ 3 & 5 \end{pmatrix}.$$

A picture of the lattice and its generators (u_1, u_2) and of the same lattice with the new basis $(u_1', 5u_2')$ is shown in Figure 35.1, where the lattice points are displayed as stars.

The invariant factor decomposition of a finitely generated module M over a PID A given by Theorem 35.31 says that

$$M_{\mathrm{tor}} \approx A/\mathfrak{a}_{r+1} \oplus \cdots \oplus A/\mathfrak{a}_m,$$

a direct sum of cyclic modules, with $(0) \neq \mathfrak{a}_{r+1} \subseteq \cdots \subseteq \mathfrak{a}_m \neq A$. Using the Chinese Remainder Theorem (Theorem 32.15), we can further decompose each module $A/\alpha_i A$ into a direct sum of modules of the form $A/p^n A$, where p is a prime in A.

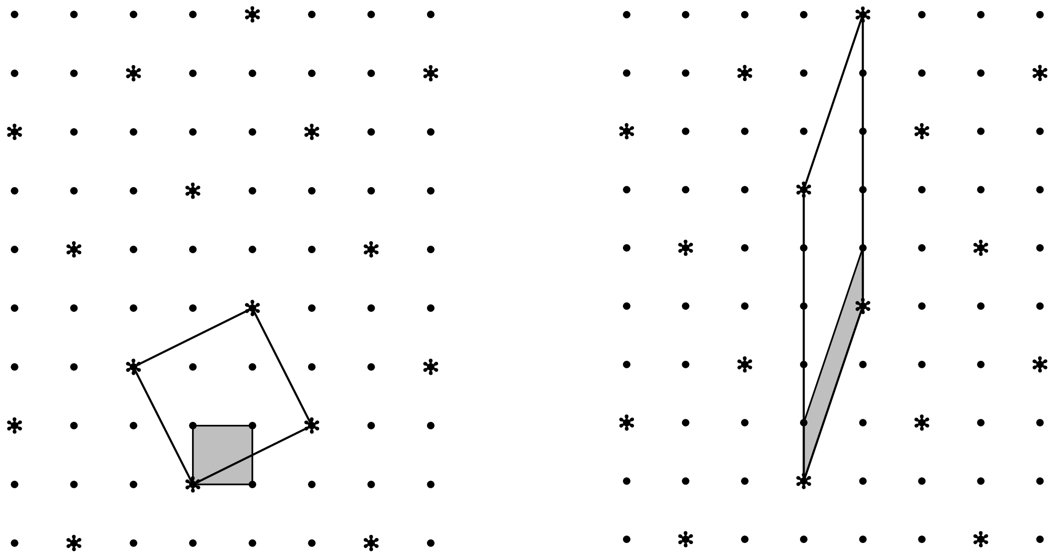

Figure 35.1: Diagonalization applied to a lattice

Theorem 35.38. *(Elementary Divisors Decomposition) Let M be a finitely generated nontrivial A-module, where A a PID. Then, M is isomorphic to the direct sum $A^r \oplus M_{\mathrm{tor}}$, where A^r is a free module and where the torsion module M_{tor} is a direct sum of cyclic modules of the form $A/p_i^{n_{i,j}}$, for some primes $p_1, \ldots, p_t \in A$ and some positive integers $n_{i,j}$, such that for each $i = 1, \ldots, t$, there is a sequence of integers*

$$1 \leq \underbrace{n_{i,1}, \ldots, n_{i,1}}_{m_{i,1}} < \underbrace{n_{i,2}, \ldots, n_{i,2}}_{m_{i,2}} < \cdots < \underbrace{n_{i,s_i}, \ldots, n_{i,s_i}}_{m_{i,s_i}},$$

with $s_i \geq 1$, and where $n_{i,j}$ occurs $m_{i,j} \geq 1$ times, for $j = 1, \ldots, s_i$. Furthermore, the irreducible elements p_i and the integers $r, t, n_{i,j}, s_i$, $m_{i,j}$ are uniquely determined.

Proof. By Theorem 35.31, we already know that $M \approx A^r \oplus M_{\mathrm{tor}}$, where r is uniquely determined, and where

$$M_{\mathrm{tor}} \approx A/\mathfrak{a}_{r+1} \oplus \cdots \oplus A/\mathfrak{a}_m,$$

a direct sum of cyclic modules, with $(0) \neq \mathfrak{a}_{r+1} \subseteq \cdots \subseteq \mathfrak{a}_m \neq A$. Then, each $\mathfrak{a}_i$ is a principal ideal of the form $\alpha_i A$, where $\alpha_i \neq 0$ and α_i is not a unit. Using the Chinese Remainder Theorem (Theorem 32.15), if we factor α_i into prime factors as

$$\alpha_i = u p_1^{k_1} \cdots p_h^{k_h},$$

with $k_j \geq 1$, we get an isomorphism

$$A/\alpha_i A \approx A/p_1^{k_1} A \oplus \cdots \oplus A/p_h^{k_h} A.$$

This implies that M_{tor} is the direct sum of modules of the form $A/p_i^{n_{i,j}}$, for some primes $p_i \in A$.

To prove uniqueness, observe that the p_i-primary component of M_{tor} is the direct sum

$$(A/p_i^{n_{i,1}}A)^{m_{i,1}} \oplus \cdots \oplus (A/p_i^{n_{i,s_i}}A)^{m_{i,s_i}},$$

and these are uniquely determined. Since $n_{i,1} < \cdots < n_{i,s_i}$, we have

$$p_i^{n_{i,s_i}}A \subseteq \cdots \subseteq p_i^{n_{i,1}}A \neq A,$$

Proposition 35.30 implies that the irreducible elements p_i and $n_{i,j}$, s_i, and $m_{i,j}$ are unique. □

In view of Theorem 35.38, we make the following definition.

Definition 35.13. Given a finitely generated module M over a PID A as in Theorem 35.38, the ideals $p_i^{n_{i,j}}A$ are called the *elementary divisors* of M, and the $m_{i,j}$ are their *multiplicities*. The ideal (0) is also considered to be an elementary divisor and r is its multiplicity.

Remark: Theorem 35.38 shows how the elementary divisors are obtained from the invariant factors: the elementary divisors are the prime power factors of the invariant factors.

Conversely, we can get the invariant factors from the elementary divisors. We may assume that M is a torsion module. Let

$$m = \max_{1\leq i\leq t}\{m_{i,1} + \cdots + m_{i,s_i}\},$$

and construct the $t \times m$ matrix $C = (c_{ij})$ whose ith row is the sequence

$$\underbrace{n_{i,s_i}, \ldots, n_{i,s_i}}_{m_{i,s_i}}, \ldots, \underbrace{n_{i,2}, \ldots, n_{i,2}}_{m_{i,2}}, \underbrace{n_{i,1}, \ldots, n_{i,1}}_{m_{i,1}}, 0, \ldots, 0,$$

padded with 0's if necessary to make it of length m. Then, the jth invariant factor is

$$\alpha_j A = p_1^{c_{1j}} p_2^{c_{2j}} \cdots p_t^{c_{tj}} A.$$

Observe that because the last column contains at least one prime, the α_i are not units, and $\alpha_m \mid \alpha_{m-1} \mid \cdots \mid \alpha_1$, so that $\alpha_1 A \subseteq \cdots \subseteq \alpha_{m-1}A \subseteq \alpha_m A \neq A$, as desired.

From a computational point of view, finding the elementary divisors is usually practically impossible, because it requires factoring. For example, if $A = K[X]$ where K is a field, such as $K = \mathbb{R}$ or $K = \mathbb{C}$, factoring amounts to finding the roots of a polynomial, but by Galois theory, in general, this is not algorithmically doable. On the other hand, the invariant factors can be computed using elementary row and column operations.

It can also be shown that A and the modules of the form A/p^nA are indecomposable (with $n > 0$). A module M is said to be *indecomposable* if M cannot be written as a direct sum of two nonzero proper submodules of M. For a proof, see Bourbaki [26] (Chapter VII, Section 4, No. 8, Proposition 8). Theorem 35.38 shows that a finitely generated module over a PID is a direct sum of indecomposable modules.

In Chapter 36 we apply the structure theorems for finitely generated (torsion) modules to the $K[X]$-module E_f associated with an endomorphism f on a vector space E. First, we need to understand the process of extension of the ring of scalars.

35.6 Extension of the Ring of Scalars

The need to extend the ring of scalars arises, in particular when dealing with eigenvalues. First we need to define how to restrict scalar multiplication to a subring. The situation is that we have two rings A and B, a B-module M, and a ring homomorphism $\rho\colon A \to B$. The special case that arises often is that A is a subring of B (B could be a field) and ρ is the inclusion map. Then we can make M into an A-module by defining the scalar multiplication $\cdot\colon A \times M \to M$ as follows.

Definition 35.14. Given two rings A and B and a ring homomorphism $\rho\colon A \to B$, any B-module M can made into an A-module denoted by $\rho_*(M)$, by defining scalar multiplication by any element of A as follows:

$$a \cdot x = \rho(a)x, \quad \text{for all } a \in A \text{ and all } x \in M.$$

In particular, viewing B as a B-module, we obtain the A-module $\rho_*(B)$.

If M and N are two B-modules and if $f\colon M \to N$ is a B-linear map, the map f is a homomorphism $f\colon \rho_*(M) \to \rho_*(N)$ of the abelian groups $\rho_*(M)$ and $\rho_*(N)$. This map is also A-linear, because for all $u \in M$ and all $a \in A$, by definition of the scalar multiplication by elements of A, we have

$$f(a \cdot u) = f(\rho(a)u) = \rho(a)f(u) = a \cdot f(u).$$

The map $f\colon \rho_*(M) \to \rho_*(N)$ viewed as an A-linear map is denoted by $\rho_*(f)$. As homomorphisms of abelian groups, the maps $f\colon M \to N$ and $\rho_*(f)\colon \rho_*(M) \to \rho_*(N)$ are identical, but f is a B-linear map whereas $\rho_*(f)$ is an A-linear map.

Now we can describe the process of scalar extension. Given any A-module M, we make $\rho_*(B) \otimes_A M$ into a (left) B-module as follows: for every $\beta \in B$, let $\mu_\beta\colon \rho_*(B) \times M \to \rho_*(B) \otimes_A M$ be given by

$$\mu_\beta(\beta', x) = (\beta\beta') \otimes x.$$

The map μ_β is bilinear so it induces a linear map $\mu_\beta\colon \rho_*(B) \otimes_A M \to \rho_*(B) \otimes_A M$ such that

$$\mu_\beta(\beta' \otimes x) = (\beta\beta') \otimes x.$$

If we define the scalar multiplication $\cdot\colon B \times (\rho_*(B) \otimes_A M) \to \rho_*(B) \otimes_A M$ by

$$\beta \cdot z = \mu_\beta(z), \quad \text{for all } \beta \in B \text{ and all } z \in \rho_*(B) \otimes_A M,$$

then it is easy to check that the axioms M1, M2, M3, M4 hold. Let us check M2 and M3. We have

$$\begin{aligned}\mu_{\beta_1+\beta_2}(\beta' \otimes x) &= (\beta_1 + \beta_2)\beta' \otimes x \\ &= (\beta_1\beta' + \beta_2\beta') \otimes x \\ &= \beta_1\beta' \otimes x + \beta_2\beta' \otimes x \\ &= \mu_{\beta_1}(\beta' \otimes x) + \mu_{\beta_2}(\beta' \otimes x)\end{aligned}$$

and

$$\begin{aligned}\mu_{\beta_1\beta_2}(\beta' \otimes x) &= \beta_1\beta_2\beta' \otimes x \\ &= \mu_{\beta_1}(\beta_2\beta' \otimes x) \\ &= \mu_{\beta_1}(\mu_{\beta_2}(\beta' \otimes x)).\end{aligned}$$

Definition 35.15. Given two rings A and B and a ring homomorphism $\rho\colon A \to B$, for any A-module M, with the scalar multiplication by elements of B given by

$$\beta \cdot (\beta' \otimes x) = (\beta\beta') \otimes x, \quad \beta, \beta' \in B,\ x \in M,$$

the tensor product $\rho_*(B) \otimes_A M$ is a B-module denoted by $\rho^*(M)$, or $M_{(B)}$ when ρ is the inclusion of A into B. The B-module $\rho^*(M)$ is sometimes called the *module induced from M by extension to B of the ring of scalars through ρ.*

Here is a specific example of Definition 35.15. Let $A = \mathbb{R}$, $B = \mathbb{C}$ and ρ be the inclusion map of $\mathbb{R}$ into $\mathbb{C}$, i.e. $\rho\colon \mathbb{R} \to \mathbb{C}$ with $\rho(a) = a$ for $a \in \mathbb{R}$. Let M be an $\mathbb{R}$-module. The field $\mathbb{C}$ is a $\mathbb{C}$-module, and when we restrict scalar multiplication by scalars $\lambda \in \mathbb{R}$, we obtain the $\mathbb{R}$-module $\rho_*(\mathbb{C})$ (which, as an abelian group, is just $\mathbb{C}$). Form $\rho_*(\mathbb{C}) \otimes_\mathbb{R} M$. This is an $\mathbb{R}$-module where typical elements have the form $\sum_{i=1}^n a_i(z_i \otimes m_i)$, $a_i \in \mathbb{R}$, $z_i \in \mathbb{C}$, and $m_i \in M$. Since

$$a_i(z_i \otimes m_i) = a_iz_i \otimes m_i$$

and since $a_iz_i \in \mathbb{C}$ and any element of $\mathbb{C}$ is obtained this way (let $a_i = 1$), the elements of $\rho_*(\mathbb{C}) \otimes_\mathbb{R} M$ can be written as

$$\sum_{i=1}^n z_i \otimes m_i, \quad z_i \in \mathbb{C},\ m_i \in M.$$

We want to make $\rho_*(\mathbb{C}) \otimes_\mathbb{R} M$ into a $\mathbb{C}$-module, denoted $\rho^*(M)$, and thus must describe how a complex number β acts on $\sum_{i=1}^n z_i \otimes m_i$. By linearity, it is enough to determine how $\beta = u + iv$ acts on a generator $z \otimes m$, where $z = x + iy$ and $m \in M$. The action is given by

$$\beta \cdot (z \otimes m) = \beta z \otimes m = (u + iv)(x + iy) \otimes m = (ux - vy + i(uy + vx)) \otimes m,$$

since complex multiplication only makes sense over $\mathbb{C}$.

We claim that $\rho^*(M)$ is isomorphic to the $\mathbb{C}$-module $M \times M$ with addition defined by

$$(u_1, v_1) + (u_2, v_2) = (u_1 + u_2, v_1 + v_2)$$

and scalar multiplication by $\lambda + i\mu \in \mathbb{C}$ as

$$(\lambda + i\mu) \cdot (u, v) = (\lambda u - \mu v, \lambda v + \mu u).$$

Define the map $\alpha_0 \colon \rho_*(\mathbb{C}) \times M \to M \times M$ by

$$\alpha_0(\lambda + i\mu, u) = (\lambda u, \mu u).$$

It is easy to check that α_0 is $\mathbb{R}$-linear, so we obtain an $\mathbb{R}$-linear map $\alpha \colon \rho_*(\mathbb{C}) \otimes_{\mathbb{R}} M \to M \times M$ such that

$$\alpha((\lambda + i\mu) \otimes u) = (\lambda u, \mu u).$$

We also define the map $\beta \colon M \times M \to \rho_*(\mathbb{C}) \otimes_{\mathbb{R}} M$ by

$$\beta(u, v) = 1 \otimes u + i \otimes v.$$

Again, it is clear that this map is $\mathbb{R}$-linear. We can now check that α and β are mutual inverses. We have

$$\alpha(\beta(u, v)) = \alpha(1 \otimes u + i \otimes v) = \alpha(1 \otimes u) + \alpha(i \otimes v) = (u, 0) + (0, v) = (u, v),$$

and on generators,

$$\beta(\alpha((\lambda + i\mu) \otimes u)) = \beta(\lambda u, \mu u) = 1 \otimes \lambda u + i \otimes \mu u = \lambda \otimes u + i\mu \otimes u = (\lambda + i\mu) \otimes u.$$

Therefore, $\rho_*(\mathbb{C}) \otimes_{\mathbb{R}} M$ and $M \times M$ are isomorphic as $\mathbb{R}$-module. However, the isomorphism α is also an isomorphism of $\mathbb{C}$-modules. This is because in $\rho_*(\mathbb{C}) \otimes_{\mathbb{R}} M$, on generators we have

$$(\lambda + i\mu) \cdot ((x + iy) \otimes u) = (\lambda + i\mu)(x + iy) \otimes u = (\lambda x - \mu y + i(\lambda y + \mu x)) \otimes u,$$

so

$$\begin{aligned}\alpha((\lambda + i\mu) \cdot ((x + iy) \otimes u) &= \alpha((\lambda x - \mu y + i(\lambda y + \mu x)) \otimes u)\\ &= ((\lambda x - \mu y)u, (\lambda y + \mu x)u),\end{aligned}$$

and by definition of the scalar multiplication by elements of $\mathbb{C}$ on $M \times M$

$$(\lambda + i\mu) \cdot \alpha((x + iy) \otimes u) = (\lambda + i\mu) \cdot (xu, yu) = ((\lambda x - \mu y)u, (\lambda y + \mu x)u).$$

Therefore, α is isomorphism between the $\mathbb{C}$-modules $\rho^*(M) = \rho_*(\mathbb{C}) \otimes_{\mathbb{R}} M$ and $M \times M$.

The above process of ring extension can also be applied to linear maps. We have the following proposition whose proof is given in Bourbaki [25] (Chapter II, Section 5, Proposition 1).

Proposition 35.39. *Given a ring homomomorphism $\rho\colon A \to B$ and given any A-module M, the map $\varphi\colon M \to \rho_*(\rho^*(M))$ given by $\varphi(x) = 1 \otimes_A x$ is A-linear and $\varphi(M)$ spans the B-module $\rho^*(M)$. For every B-module N, and for every A-linear map $f\colon M \to \rho_*(N)$, there is a unique B-linear map*

$$\overline{f}\colon \rho^*(M) \to N$$

such that

$$\rho_*(\overline{f}) \circ \varphi = f$$

as in the following commutative diagram

$$\begin{tikzcd}
M \arrow[r, "\varphi"] \arrow[dr, "f"'] & \rho_*(\rho^*(M)) \arrow[d, "\rho_*(\overline{f})"] \\
& \rho_*(N)
\end{tikzcd}$$

or equivalently,

$$\overline{f}(1 \otimes_A x) = f(x), \quad \text{for all } x \in M.$$

As a consequence of Proposition 35.39, we obtain the following result.

Proposition 35.40. *Given a ring homomomorphism $\rho\colon A \to B$, for any two A-modules M an N, for every A-linear map $f\colon M \to N$, there is a unique B-linear map $\rho^*(f)\colon \rho^*(M) \to \rho^*(N)$ (also denoted $\overline{f}$) given by*

$$\rho^*(f) = \mathrm{id}_B \otimes f,$$

such that the following diagam commutes:

$$\begin{tikzcd}
M \arrow[r, "\varphi_M"] \arrow[d, "f"'] & \rho_*(\rho^*(M)) \arrow[d, "\rho_*(\rho^*(f))"] \\
N \arrow[r, "\varphi_N"'] & \rho_*(\rho^*(N))
\end{tikzcd}$$

Proof. Apply Proposition 35.40 to the A-linear map $\varphi_N \circ f$. □

If S spans the module M, it is clear that $\varphi(S)$ spans $\rho^*(M)$. In particular, if M is finitely generated, so if $\rho^*(M)$. Bases of M also extend to bases of $\rho^*(M)$.

Proposition 35.41. *Given a ring homomomorphism $\rho\colon A \to B$, for any A-module M, if $(u_1, \ldots, u_n)$ is a basis of M, then $(\varphi(u_1), \ldots, \varphi(u_n))$ is a basis of $\rho^*(M)$, where φ is the A-linear map $\varphi\colon M \to \rho_*(\rho^*(M))$ given by $\varphi(x) = 1 \otimes_A x$. Furthermore, if ρ is injective, then so is φ.*

Proof. The first assertion follows immediately from Proposition 35.13, since it asserts that every element z of $\rho^*(M) = \rho_*(B) \otimes_A M$ can be written in a unique way as

$$z = b_1 \otimes u_1 + \cdots + b_n \otimes u_n = b_1(1 \otimes u_1) + \cdots + b_n(1 \otimes u_n),$$

and $\varphi(u_i) = 1 \otimes u_i$. Next, if ρ is injective, by definition of the scalar multiplication in the A-module $\rho_*(\rho^*(M))$, we have $\varphi(a_1u_1 + \cdots + a_nu_n) = 0$ iff

$$\rho(a_1)\varphi(u_1) + \cdots + \rho(a_n)\varphi(u_n) = 0,$$

and since $(\varphi(u_1), \ldots, \varphi(u_n))$ is a basis of $\rho^*(M)$, we must have $\rho(a_i) = 0$ for $i = 1, \ldots, n$, which (by injectivity of ρ) implies that $a_i = 0$ for $i = 1, \ldots, n$. Therefore, φ is injective. □

In particular, if A is a subring of B, then ρ is the inclusion map and Proposition 35.41 shows that a basis of M becomes a basis of $M_{(B)}$ and that M is embedded into $M_{(B)}$. It is also easy to see that if M and N are two free A-modules and $f\colon M \to N$ is a linear map represented by the matrix X with respect to some bases $(u_1, \ldots, u_n)$ of M and $(v_1, \ldots, v_m)$ of N, then the B-linear map $\overline{f}$ is also represented by the matrix X over the bases $(\varphi(u_1), \ldots, \varphi(u_n))$ and $(\varphi(v_1), \ldots, \varphi(v_m))$.

Proposition 35.41 yields another proof of the fact that any two bases of a free A-modules have the same cardinality. Indeed, if $\mathfrak{m}$ is a maximal ideal in the ring A, then we have the quotient ring homomorphism $\pi\colon A \to A/\mathfrak{m}$, and we get the $A/\mathfrak{m}$-module $\pi^*(M)$. If M is free, any basis $(u_1, \ldots, u_n)$ of M becomes the basis $(\varphi(u_1), \ldots, \varphi(u_n))$ of $\pi^*(M)$; but $A/\mathfrak{m}$ is a field, so the dimension n is uniquely determined. This argument also applies to an infinite basis $(u_i)_{i\in I}$. Observe that by Proposition 35.14, we have an isomorphism

$$\pi^*(M) = (A/\mathfrak{m}) \otimes_A M \approx M/\mathfrak{m}M,$$

so $M/\mathfrak{m}M$ is a vector space over the field $A/\mathfrak{m}$, which is the argument used in Theorem 35.1.

Proposition 35.42. *Given a ring homomomorphism $\rho\colon A \to B$, for any two A-modules M and N, there is a unique isomorphism*

$$\rho^*(M) \otimes_B \rho^*(N) \approx \rho^*(M \otimes_A N),$$

such that $(1 \otimes u) \otimes (1 \otimes v) \mapsto 1 \otimes (u \otimes v)$, for all $u \in M$ and all $v \in N$.

The proof uses identities from Proposition 33.13. It is not hard but it requires a little gymnastic; a good exercise for the reader.

Chapter 36

The Rational Canonical Form and Other Normal Forms

36.1 The Torsion Module Associated With An Endomorphism

We saw in Section 7.7 that given a linear map $f\colon E \to E$ from a K-vector space E into itself, we can define a scalar multiplication $\cdot\colon K[X] \times E \to E$ that makes E into a $K]X]$-module. If E is finite-dimensional, this $K[X]$-module denoted by E_f is a torsion module, and the main results of this chapter yield important direct sum decompositions of E into subspaces invariant under f.

Recall that given any polynomial $p(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n$ with coefficients in the field K, we define the *linear map* $p(f)\colon E \to E$ by

$$p(f) = a_0f^n + a_1f^{n-1} + \cdots + a_n\mathrm{id},$$

where $f^k = f \circ \cdots \circ f$, the k-fold composition of f with itself. Note that

$$p(f)(u) = a_0f^n(u) + a_1f^{n-1}(u) + \cdots + a_nu,$$

for every vector $u \in E$. Then, we define the scalar multiplication $\cdot\colon K[X] \times E \to E$ by polynomials as follows: for every polynomial $p(X) \in K[X]$, for every $u \in E$,

$$p(X) \cdot u = p(f)(u).^{1}$$

It is easy to verify that this scalar multiplication satisfies the axioms M1, M2, M3, M4:

$$\begin{aligned} p \cdot (u + v) &= p \cdot u + p \cdot v \\ (p + q) \cdot u &= p \cdot u + q \cdot u \\ (pq) \cdot u &= p \cdot (q \cdot u) \\ 1 \cdot u &= u, \end{aligned}$$

[1] If necessary to avoid confusion, we use the notion $p(X) \cdot_f u$ instead of $p(X) \cdot u$.

for all $p, q \in K[X]$ and all $u, v \in E$. Thus, with this new scalar multiplication, E is a $K[X]$-module denoted by E_f.

If $p = \lambda$ is just a scalar in K (a polynomial of degree 0), then

$$\lambda \cdot u = (\lambda \mathrm{id})(u) = \lambda u,$$

which means that K acts on E by scalar multiplication as before. If $p(X) = X$ (the monomial X), then

$$X \cdot u = f(u).$$

Since K is a field, the ring $K[X]$ is a PID.

If E is finite-dimensional, say of dimension n, since K is a subring of $K[X]$ and since E is finitely generated over K, the $K[X]$-module E_f is finitely generated over $K[X]$. Furthermore, E_f is a torsion module. This follows from the Cayley-Hamilton Theorem (Theorem 7.15), but this can also be shown in an elementary fashion as follows. The space $\mathrm{Hom}(E, E)$ of linear maps of E into itself is a vector space of dimension n^2, therefore the $n^2 + 1$ linear maps

$$\mathrm{id}, f, f^2, \ldots, f^{n^2}$$

are linearly dependent, which yields a nonzero polynomial q such that $q(f) = 0$.

We can now translate notions defined for modules into notions for endomorphisms of vector spaces.

1. To say that U is a submodule of E_f means that U is a subspace of E invariant under f; that is, $f(U) \subseteq U$.

2. To say that V is a cyclic submodule of E_f means that there is some vector $u \in V$, such that V is spanned by $(u, f(u), \ldots, f^k(u), \ldots)$. If E has finite dimension n, then V is spanned by $(u, f(u), \ldots, f^k(u))$ for some $k \leq n - 1$. We say that V is a *cyclic subspace for f with generator u*. Sometimes, V is denoted by $Z(u; f)$.

3. To say that the ideal $\mathfrak{a} = (p(X))$ (with $p(X)$ a monic polynomial) is the annihilator of the submodule V means that $p(f)(u) = 0$ for all $u \in V$, and we call p the *minimal polynomial* of V.

4. Suppose E_f is cyclic and let $\mathfrak{a} = (q)$ be its annihilator, where

$$q(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0.$$

Then, there is some vector u such that $(u, f(u), \ldots, f^k(u))$ span E_f, and because q is the minimal polynomial of E_f, we must have $k = n - 1$. The fact that $q(f) = 0$ implies that

$$f^n(u) = -a_0 u - a_1 f(u) - \cdots - a_{n-1} f^{n-1}(u),$$

and so f is represented by the following matrix known as the *companion matrix* of $q(X)$:

$$U = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ddots & 0 & -a_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}.$$

It is an easy exercise to prove that the characteristic polynomial $\chi_U(X)$ of U gives back $q(X)$:

$$\chi_U(X) = q(X).$$

We will need the following proposition to characterize when two linear maps are similar.

Proposition 36.1. *Let $f\colon E \to E$ and $f'\colon E' \to E'$ be two linear maps over the vector spaces E and E'. A linear map $g\colon E \to E'$ can be viewed as a linear map between the $K[X]$-modules E_f and $E_{f'}$ iff*

$$g \circ f = f' \circ g.$$

Proof. First, suppose g is $K[X]$-linear. Then, we have

$$g(p \cdot_f u) = p \cdot_{f'} g(u)$$

for all $p \in K[X]$ and all $u \in E$, so for $p = X$ we get

$$g(p \cdot_f u) = g(X \cdot_f u) = g(f(u))$$

and

$$p \cdot_{f'} g(u) = X \cdot_{f'} g(u) = f'(g(u)),$$

which means that $g \circ f = f' \circ g$.

Conversely, if $g \circ f = f' \circ g$, we prove by induction that

$$g \circ f^n = f'^n \circ g, \quad \text{for all } n \geq 1.$$

Indeed, we have

$$\begin{aligned} g \circ f^{n+1} &= g \circ f^n \circ f \\ &= f'^n \circ g \circ f \\ &= f'^n \circ f' \circ g \\ &= f'^{n+1} \circ g, \end{aligned}$$

establishing the induction step. It follows that for any polynomial $p(X) = \sum_{k=0}^{n} a_k X^k$, we have

$$\begin{aligned} g(p(X) \cdot_f u) &= g\Big(\sum_{k=0}^{n} a_k f^k(u)\Big) \\ &= \sum_{k=0}^{n} a_k g \circ f^k(u) \\ &= \sum_{k=0}^{n} a_k f'^k \circ g(u) \\ &= \Big(\sum_{k=0}^{n} a_k f'^k\Big)(g(u)) \\ &= p(X) \cdot_{f'} g(u), \end{aligned}$$

so, g is indeed $K[X]$-linear. □

Definition 36.1. We say that the linear maps $f\colon E \to E$ and $f'\colon E' \to E'$ are *similar* iff there is an isomorphism $g\colon E \to E'$ such that

$$f' = g \circ f \circ g^{-1},$$

or equivalently,

$$g \circ f = f' \circ g.$$

Then, Proposition 36.1 shows the following fact:

Proposition 36.2. *With notation of Proposition 36.1, two linear maps f and f' are similar iff g is an isomorphism between E_f and $E'_{f'}$.*

Later on, we will see that the isomorphism of finitely generated torsion modules can be characterized in terms of invariant factors, and this will be translated into a characterization of similarity of linear maps in terms of so-called similarity invariants. If f and f' are represented by matrices A and A' over bases of E and E', then f and f' are similar iff the matrices A and A' are similar (there is an invertible matrix P such that $A' = PAP^{-1}$). Similar matrices (and endomorphisms) have the same characteristic polynomial.

It turns out that there is a useful relationship between E_f and the module $K[X] \otimes_K E$. Observe that the map $\cdot\colon K[X] \times E \to E$ given by

$$p \cdot u = p(f)(u)$$

is K-bilinear, so it yields a K-linear map $\sigma\colon K[X] \otimes_K E \to E$ such that

$$\sigma(p \otimes u) = p \cdot u = p(f)(u).$$

We know from Section 35.6 that $K[X] \otimes_K E$ is a $K[X]$-module (obtained from the inclusion $K \subseteq K[X]$), which we will denote by $E[X]$. Since E is a vector space, $E[X]$ is a free $K[X]$-module, and if $(u_1, \ldots, u_n)$ is a basis of E, then $(1 \otimes u_1, \ldots, 1 \otimes u_n)$ is a basis of $E[X]$.

The free $K[X]$-module $E[X]$ is not as complicated as it looks. Over the basis $(1 \otimes u_1, \ldots, 1 \otimes u_n)$, every element $z \in E[X]$ can be written uniquely as

$$z = p_1(1 \otimes u_1) + \cdots + p_n(1 \otimes u_n) = p_1 \otimes u_1 + \cdots + p_n \otimes u_n,$$

where $p_1, \ldots, p_n$ are polynomials in $K[X]$. For notational simplicity, we may write

$$z = p_1 u_1 + \cdots + p_n u_n,$$

where $p_1, \ldots, p_n$ are viewed as coefficients in $K[X]$. With this notation, we see that $E[X]$ is isomorphic to $(K[X])^n$, which is easy to understand.

Observe that σ is $K[X]$-linear, because

$$\begin{aligned}
\sigma(q(p \otimes u)) &= \sigma((qp) \otimes u) \\
&= (qp) \cdot u \\
&= q(f)(p(f)(u)) \\
&= q \cdot (p(f)(u)) \\
&= q \cdot \sigma(p \otimes u).
\end{aligned}$$

Therefore, σ is a linear map of $K[X]$-modules, $\sigma \colon E[X] \to E_f$. Using our simplified notation, if $z = p_1 u_1 + \cdots + p_n u_n \in E[X]$, then

$$\sigma(z) = p_1(f)(u_1) + \cdots + p_n(f)(u_n),$$

which amounts to plugging f for X and evaluating. Similarly, f is a $K[X]$-linear map of E_f, because

$$\begin{aligned}
f(p \cdot u) &= f(p(f)(u)) \\
&= (fp(f))(u) \\
&= p(f)(f(u)) \\
&= p \cdot f(u),
\end{aligned}$$

where we used the fact that $fp(f) = p(f)f$ because $p(f)$ is a polynomial in f. By Proposition 35.40, the linear map $f \colon E \to E$ induces a $K[X]$-linear map $\overline{f} \colon E[X] \to E[X]$ such that

$$\overline{f}(p \otimes u) = p \otimes f(u).$$

Observe that we have

$$f(\sigma(p \otimes u)) = f(p(f)(u)) = p(f)(f(u))$$

and

$$\sigma(\overline{f}(p \otimes u)) = \sigma(p \otimes f(u)) = p(f)(f(u)),$$

so we get

$$\sigma \circ \overline{f} = f \circ \sigma. \tag{$*$}$$

Using our simplified notation,

$$\overline{f}(p_1 u_1 + \cdots + p_n u_n) = p_1 f(u_1) + \cdots + p_n f(u_n).$$

Define the $K[X]$-linear map $\psi \colon E[X] \to E[X]$ by

$$\psi(p \otimes u) = (Xp) \otimes u - p \otimes f(u).$$

Observe that $\psi = X1_{E[X]} - \overline{f}$, which we abbreviate as $X1 - \overline{f}$. Using our simplified notation

$$\psi(p_1 u_1 + \cdots + p_n u_n) = X p_1 u_1 + \cdots + X p_n u_n - (p_1 f(u_1) + \cdots + p_n f(u_n)).$$

It should be noted that everything we did in Section 36.1 applies to modules over a commutative ring A, except for the statements that assume that $A[X]$ is a PID. So, if M is an A-module, we can define the $A[X]$-modules M_f and $M[X] = A[X] \otimes_A M$, except that M_f is generally not a torsion module, and all the results showed above hold. Then, we have the following remarkable result.

Theorem 36.3. *(The Characteristic Sequence) Let A be a ring and let E be an A-module. The following sequence of $A[X]$-linear maps is exact:*

$$\begin{tikzcd} 0 \arrow[r] & E[X] \arrow[r, "\psi"] & E[X] \arrow[r, "\sigma"] & E_f \arrow[r] & 0. \end{tikzcd}$$

This means that ψ is injective, σ is surjective, and that $\mathrm{Im}(\psi) = \mathrm{Ker}\,(\sigma)$*. As a consequence, E_f is isomorphic to the quotient of $E[X]$ by* $\mathrm{Im}(X1 - \overline{f})$*.*

Proof. Because $\sigma(1 \otimes u) = u$ for all $u \in E$, the map σ is surjective. We have

$$\begin{aligned} \sigma(X(p \otimes u)) &= X \cdot \sigma(p \otimes u) \\ &= f(\sigma(p \otimes u)), \end{aligned}$$

which shows that

$$\sigma \circ X1 = f \circ \sigma = \sigma \circ \overline{f},$$

using $(*)$. This implies that

$$\begin{aligned} \sigma \circ \psi &= \sigma \circ (X1 - \overline{f}) \\ &= \sigma \circ X1 - \sigma \circ \overline{f} \\ &= \sigma \circ \overline{f} - \sigma \circ \overline{f} = 0, \end{aligned}$$

and thus, $\mathrm{Im}(\psi) \subseteq \mathrm{Ker}\,(\sigma)$. It remains to prove that $\mathrm{Ker}\,(\sigma) \subseteq \mathrm{Im}(\psi)$.

Since the monomials X^k form a basis of $A[X]$, by Proposition 35.13 (with the roles of M and N exchanged), every $z \in E[X] = A[X] \otimes_A E$ has a unique expression as

$$z = \sum_k X^k \otimes u_k,$$

for a family (u_k) of finite support of $u_k \in E$. If $z \in \mathrm{Ker}\,(\sigma)$, then

$$0 = \sigma(z) = \sum_k f^k(u_k),$$

which allows us to write

$$\begin{aligned} z &= \sum_k X^k \otimes u_k - 1 \otimes 0 \\ &= \sum_k X^k \otimes u_k - 1 \otimes \Big(\sum_k f^k(u_k)\Big) \\ &= \sum_k (X^k \otimes u_k - 1 \otimes f^k(u_k)) \\ &= \sum_k (X^k(1 \otimes u_k) - \overline{f}^k(1 \otimes u_k)) \\ &= \sum_k (X^k 1 - \overline{f}^k)(1 \otimes u_k). \end{aligned}$$

Now, $X1$ and $\overline{f}$ commute, since

$$\begin{aligned} (X1 \circ \overline{f})(p \otimes u) &= (X1)(p \otimes f(u)) \\ &= (Xp) \otimes f(u) \end{aligned}$$

and

$$\begin{aligned} (\overline{f} \circ X1)(p \otimes u) &= \overline{f}((Xp) \otimes u) \\ &= (Xp) \otimes f(u), \end{aligned}$$

so we can write

$$X^k 1 - \overline{f}^k = (X1 - \overline{f})\bigg(\sum_{j=0}^{k-1} (X1)^j \overline{f}^{k-j-1}\bigg),$$

and

$$z = (X1 - \overline{f})\bigg(\sum_k \bigg(\sum_{j=0}^{k-1} (X1)^j \overline{f}^{k-j-1}\bigg)(1 \otimes u_k)\bigg),$$

which shows that $z = \psi(y)$ for some $y \in E[X]$.

Finally, we prove that ψ is injective as follows. We have

$$\begin{aligned}\psi(z) &= \psi\biggl(\sum_k X^k \otimes u_k\biggr)\\ &= (X1 - \overline{f})\biggl(\sum_k X^k \otimes u_k\biggr)\\ &= \sum_k X^{k+1} \otimes (u_k - f(u_{k+1})),\end{aligned}$$

where (u_k) is a family of finite support of $u_k \in E$. If $\psi(z) = 0$, then

$$\sum_k X^{k+1} \otimes (u_k - f(u_{k+1})) = 0,$$

and because the X^k form a basis of $A[X]$, we must have

$$u_k - f(u_{k+1}) = 0, \quad \text{for all } k.$$

Since (u_k) has finite support, there is a largest k, say $m+1$ so that $u_{m+1} = 0$, and then from

$$u_k = f(u_{k+1}),$$

we deduce that $u_k = 0$ for all k. Therefore, $z = 0$, and ψ is injective. □

Remark: The exact sequence of Theorem 36.3 yields a *presentation* of M_f.

Since $A[X]$ is a free A-module, $A[X] \otimes_A M$ is a free A-module, but $A[X] \otimes_A M$ is generally not a free $A[X]$-module. However, if M is a free module, then $M[X]$ is a free $A[X]$-module, since if $(u_i)_{i\in I}$ is a basis for M, then $(1 \otimes u_i)_{i\in I}$ is a basis for $M[X]$. This allows us to define the characterisctic polynomial $\chi_f(X)$ of an endomorphism of a free module M as

$$\chi_f(X) = \det(X1 - \overline{f}).$$

Note that to have a correct definition, we need to define the determinant of a linear map allowing the indeterminate X as a scalar, and this is what the definition of $M[X]$ achieves (among other things). Theorem 36.3 can be used to give a short proof of the Cayley-Hamilton Theorem, see Bourbaki [25] (Chapter III, Section 8, Proposition 20). Proposition 7.10 is still the crucial ingredient of the proof.

36.2 The Rational Canonical Form

Let E be a finite-dimensional vector space over a field K, and let $f\colon E \to E$ be an endomorphism of E. We know from Section 36.1 that there is a $K[X]$-module E_f associated with f, and that E_f is a finitely generated torsion module over the PID $K[X]$. In this chapter, we show how Theorems from Sections 35.4 and 35.5 yield important results about the structure of the linear map f.

Recall that the annihilator of a subspace V is an ideal (p) uniquely defined by a monic polynomial p called the *minimal polynomial* of V.

Our first result is obtained by translating the primary decomposition theorem, Theorem 35.19. It is not too surprising that we obtain again Theorem 31.10!

Theorem 36.4. *(Primary Decomposition Theorem) Let $f\colon E \to E$ be a linear map on the finite-dimensional vector space E over the field K. Write the minimal polynomial m of f as*

$$m = p_1^{r_1} \cdots p_k^{r_k},$$

where the p_i are distinct irreducible monic polynomials over K, and the r_i are positive integers. Let

$$W_i = \mathrm{Ker}\,(p_i(f)^{r_i}), \quad i = 1, \ldots, k.$$

Then

(a) $E = W_1 \oplus \cdots \oplus W_k$.

(b) Each W_i is invariant under f and the projection from W onto W_i is given by a polynomial in f.

(c) The minimal polynomial of the restriction $f \mid W_i$ of f to W_i is $p_i^{r_i}$.

Example 36.1. Let $f\colon \mathbb{R}^4 \to \mathbb{R}^4$ be defined as $f(x, y, z, w) = (x + w, y + z, y + z, x + w)$. In terms of the standard basis, f has the matrix representation

$$M = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

A basic calculation shows that $\chi_f(X) = X^2(X-2)^2$ and that $m_f(X) = X(X-2)$. The primary decomposition theorem implies that

$$\mathbb{R}^4 = W_1 \oplus W_2, \qquad W_1 = \mathrm{Ker}\,(M), \qquad W_2 = \mathrm{Ker}\,(M - 2I).$$

Note that $\mathrm{Ker}\,(M)$ corresponds to the eigenspace associated with eigenvalue 0 and has basis $([-1, 0, 0, 1], [0, -1, 1, 0])$, while $\mathrm{Ker}\,(M - 2I)$ corresponds to the eigenspace associated with eigenvalue 2 and has basis $([1, 0, 0, 1], [0, 1, 1, 0])$.

Next we apply the Invariant Factors Decomposition Theorem, Theorem 35.31, to E_f. This theorem says that E_f is isomorphic to a direct sum

$$E_f \approx K[X]/(p_1) \oplus \cdots \oplus K[X]/(p_m)$$

of $m \leq n$ cyclic modules, where the p_j are uniquely determined monic polynomials of degree at least 1, such that

$$p_m \mid p_{m-1} \mid \cdots \mid p_1.$$

Each cyclic module $K[X]/(p_i)$ is isomorphic to a cyclic subspace for f, say V_i, whose minimal polynomial is p_i.

It is customary to renumber the polynomials p_i as follows. The n polynomials $q_1, \ldots, q_n$ are defined by:

$$q_j(X) = \begin{cases} 1 & \text{if } 1 \leq j \leq n-m \\ p_{n-j+1}(X) & \text{if } n-m+1 \leq j \leq n. \end{cases}$$

Then we see that

$$q_1 \mid q_2 \mid \cdots \mid q_n,$$

where the first $n-m$ polynomials are equal to 1, and we have the direct sum

$$E = E_1 \oplus \cdots \oplus E_n,$$

where E_i is a cyclic subspace for f whose minimal polynomial is q_i. In particular, $E_i = (0)$ for $i = 1, \ldots, n-m$. Theorem 35.31 also says that the minimal polynomial of f is $q_n = p_1$. We sum all this up in the following theorem.

Theorem 36.5. *(Cyclic Decomposition Theorem, First Version) Let $f \colon E \to E$ be an endomorphism on a K-vector space of dimension n. There exist n monic polynomials $q_1, \ldots, q_n \in K[X]$ such that*

$$q_1 \mid q_2 \mid \cdots \mid q_n,$$

and E is the direct sum

$$E = E_1 \oplus \cdots \oplus E_n$$

of cyclic subspaces $E_i = Z(u_i; f)$ for f, such that the minimal polynomial of the restriction of f to E_i is q_i. The polynomials q_i satisfying the above conditions are unique, and q_n is the minimal polynomial of f.

In view of translation point (4) at the beginning of Section 36.1, we know that over the basis

$$(u_i, f(u_i), \ldots, f^{n_i - 1}(u_i))$$

of the cyclic subspace $E_i = Z(u_i; f)$, with $n_i = \deg(q_i)$, the matrix of the restriction of f to E_i is the *companion matrix* of $p_i(X)$, of the form

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ddots & 0 & -a_{n_i-2} \\ 0 & 0 & 0 & \cdots & 1 & -a_{n_i-1} \end{pmatrix}.$$

If we put all these bases together, we obtain a block matrix whose blocks are of the above form. Therefore, we proved the following result.

Theorem 36.6. *(Rational Canonical Form, First Version) Let $f\colon E \to E$ be an endomorphism on a K-vector space of dimension n. There exist n monic polynomials $q_1, \ldots, q_n \in K[X]$ such that*

$$q_1 \mid q_2 \mid \cdots \mid q_n,$$

with $q_1 = \cdots = q_{n-m} = 1$, and a basis of E such that the matrix M of f is a block matrix of the form

$$M = \begin{pmatrix} M_{n-m+1} & 0 & \cdots & 0 & 0 \\ 0 & M_{n-m+2} & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & M_{n-1} & 0 \\ 0 & 0 & \cdots & 0 & M_n \end{pmatrix},$$

where each M_i is the companion matrix of q_i. The polynomials q_i satisfying the above conditions are unique, and q_n is the minimal polynomial of f.

Definition 36.2. A matrix M as in Theorem 36.6 is called a matrix in *rational form*. The polynomials $q_1, \ldots, q_n$ arising in Theorems 36.5 and 36.6 are called the *similarity invariants* (or *invariant factors*) of f.

Theorem 36.6 shows that every matrix is similar to a matrix in rational form. Such a matrix is unique.

Example 1 continued: We will calculate the rational canonical form for $f(x, y, z, w) = (x + w, y + z, y + z, x + w)$. The difficulty in finding the rational canonical form lies in determining the invariant factors q_1, q_2, q_3, q_4. As we will shortly discover, the invariant factors of f correspond to the invariant factors of $XI - M$. See Propositions 36.8 and 36.11. The invariant factors of $XI - M$ are found by converting $XI - M$ to Smith normal form. Section 36.5 describes an algorithmic procedure for computing the Smith normal form of a matrix. By applying the methodology of Section 36.5, we find that Smith normal form for

$XI - M$ is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & X(X-2) & 0 \\ 0 & 0 & 0 & X(X-2) \end{pmatrix}.$$

Thus the invariant factors of f are $q_1 = 1 = q_2$, $q_3 = X(X-2) = q_4$, and Theorem 36.5 implies that

$$\mathbb{R}^4 = E_1 \oplus E_2,$$

where $E_1 = Z(u_1, f) \cong \mathbb{R}[X]/(X(X-2))$ and $E_2 = Z(u_2, f) \cong \mathbb{R}[X]/(X(X-2))$. The subspace E_1 has basis (u_1, Mu_1) where $u_1 = (1, 0, 1, 0)$ and $Mu_1 = (1, 1, 1, 1)$, while the subspace E_2 has basis (u_2, Mu_2) where $u_2 = (0, 0, 1, 0)$ and $Mu_2 = (0, 1, 1, 0)$. Theorem 36.6 implies that rational canonical form of $M(f)$ is

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 \end{pmatrix}.$$

By Proposition 36.2, two linear maps f and f' are similar iff there is an isomorphism between E_f and $E'_{f'}$, and thus by the uniqueness part of Theorem 35.31, iff they have the same similarity invariants $q_1, \ldots, q_n$.

Proposition 36.7. *If E and E' are two finite-dimensional vector spaces and if $f \colon E \to E$ and $f' \colon E' \to E'$ are two linear maps, then f and f' are similar iff they have the same similarity invariants.*

The effect of extending the field K to a field L is the object of the next proposition.

Proposition 36.8. *Let $f \colon E \to E$ be a linear map on a K-vector space E, and let $(q_1, \ldots, q_n)$ be the similarity invariants of f. If L is a field extension of K (which means that $K \subseteq L$), and if $E_{(L)} = L \otimes_K E$ is the vector space obtained by extending the scalars, and $f_{(L)} = 1_L \otimes f$ the linear map of $E_{(L)}$ induced by f, then the similarity invariants of $f_{(L)}$ are $(q_1, \ldots, q_n)$ viewed as polynomials in $L[X]$.*

Proof. We know that E_f is isomorphic to the direct sum

$$E_f \approx K[X]/(q_1 K[X]) \oplus \cdots \oplus K[X]/(q_n K[X]),$$

so by tensoring with $L[X]$ and using Propositions 35.12 and 33.13, we get

$$\begin{aligned} L[X] \otimes_{K[X]} E_f &\approx L[X] \otimes_{K[X]} (K[X]/(q_1 K[X]) \oplus \cdots \oplus K[X]/(q_n K[X])) \\ &\approx L[X] \otimes_{K[X]} (K[X]/(q_1 K[X])) \oplus \cdots \oplus L[X] \otimes_{K[X]} (K[X]/(q_n K[X])) \\ &\approx (K[X]/(q_1 K[X])) \otimes_{K[X]} L[X] \oplus \cdots \oplus (K[X]/(q_n K[X])) \otimes_{K[X]} L[X]. \end{aligned}$$

However, by Proposition 35.14, we have isomorphisms

$$(K[X]/(q_iK[X])) \otimes_{K[X]} L[X] \approx L[X]/(q_iL[X]),$$

so we get

$$L[X] \otimes_{K[X]} E_f \approx L[X]/(q_1L[X]) \oplus \cdots \oplus L[X]/(q_nL[X]).$$

Since E_f is a $K[X]$-module, the $L[X]$ module $L[X] \otimes_{K[X]} E_f$ is the module obtained from E_f by the ring extension $K[X] \subseteq L[X]$. The L-module $E_{(L)} = L \otimes_K E$ becomes the $L[X]$-module $E_{(L)f_{(L)}}$ where

$$f_{(L)} = \mathrm{id}_L \otimes_K f.$$

We have the following proposition

Proposition 36.9. *For any field extension $K \subseteq L$, and any linear map $f\colon E \to E$ where E is a K-vector space, there is an isomorphism between the $L[X]$-modules $L[X] \otimes_{K[X]} E_f$ and $E_{(L)f_{(L)}}$.*

Proof. First we define the map $\alpha\colon L \times E \to L[X] \otimes_{K[X]} E_f$ by

$$\alpha(\lambda, u) = \lambda \otimes_{K[X]} u.$$

It is immediately verified that α is K-bilinear, so we obtain a K-linear map $\widetilde{\alpha}\colon L \otimes_K E \to L[X] \otimes_{K[X]} E_f$. Now $E_{(L)} = L \otimes_K E$ is a $L[X]$-module $(L \otimes_K E)_{f(L)}$, and let us denote this scalar multiplication by $\odot$. To describe $\odot$ it is enough to define how a monomial $aX^k \in L[X]$ acts on a generator $(\lambda \otimes_K u) \in L \otimes_K E$. We have

$$\begin{aligned} aX^k \odot (\lambda \otimes_K u) &= a(\mathrm{id}_L \otimes_K f)^k(\lambda \otimes_K u) \\ &= a(\lambda \otimes_K f^k(u)) \\ &= a\lambda \otimes_K f^k(u). \end{aligned}$$

We claim that $\widetilde{\alpha}$ is actually $L[X]$-linear. Indeed, we have

$$\begin{aligned} \widetilde{\alpha}(aX^k \odot (\lambda \otimes_K u)) &= \widetilde{\alpha}(a\lambda \otimes_K f^k(u)) \\ &= a\lambda \otimes_{K[X]} f^k(u), \end{aligned}$$

and by the definition of scalar multiplication in the $K[X]$-module E_f, we have $f^k(u) = X^k \cdot_f u$, so we have

$$\begin{aligned} \widetilde{\alpha}(aX^k \odot (\lambda \otimes_K u)) &= a\lambda \otimes_{K[X]} f^k(u) \\ &= a\lambda \otimes_{K[X]} X^k \cdot_f u \\ &= X^k \cdot (a\lambda \otimes_{K[X]} u) \\ &= aX^k \cdot (\lambda \otimes_{K[X]} u), \end{aligned}$$

which shows that $\widetilde{\alpha}$ is $L[X]$-linear.

We also define the map $\beta\colon L[X] \times E_f \to (L \otimes_K E)_{f_{(L)}}$ by

$$\beta(q(X), u) = q(X) \odot (1 \otimes_K u).$$

Using a computation similar to the computation that we just performed, we can check that β is $K[X]$-bilinear so we obtain a map $\widetilde{\beta}\colon L[X] \otimes_{K[X]} E_f \to (L \otimes_K E)_{f_{(L)}}$. To finish the proof, it suffices to prove that $\widetilde{\alpha} \circ \widetilde{\beta}$ and $\widetilde{\beta} \circ \widetilde{\alpha}$ are the identity on generators. We have

$$\widetilde{\alpha} \circ \widetilde{\beta}(q(X) \otimes_{K[X]} u) = \widetilde{\alpha}(q(X) \odot (1 \otimes_K u)) = q(X) \cdot (1 \otimes_{K[X]} u)) = q(X) \otimes_{K[X]} u,$$

and

$$\widetilde{\beta} \circ \widetilde{\alpha}(\lambda \otimes_K u) = \widetilde{\beta}(\lambda \otimes_{K[X]} u) = \lambda \odot (1 \otimes_K u) = \lambda \otimes_K u,$$

which finishes the proof. □

By Proposition 36.9,

$$E_{(L)f_{(L)}} \approx L[X] \otimes_{K[X]} E_f \approx L[X]/(q_1 L[X]) \oplus \cdots \oplus L[X]/(q_n L[X]),$$

which shows that $(q_1, \ldots, q_n)$ are the similarity invariants of $f_{(L)}$. □

Proposition 36.8 justifies the terminology "invariant" in similarity invariants. Indeed, under a field extension $K \subseteq L$, the similarity invariants of $f_{(L)}$ remain the same. This is not true of the elementary divisors, which depend on the field; indeed, an irreducible polynomial $p \in K[X]$ may split over $L[X]$. Since q_n is the minimal polynomial of f, the above reasoning also shows that the minimal polynomial of $f_{(L)}$ remains the same under a field extension.

Proposition 36.8 has the following corollary.

Proposition 36.10. *Let K be a field and let $L \supseteq K$ be a field extension of K. For any two square matrices A and B over K, if there is an invertible matrix Q over L such that $B = QAQ^{-1}$, then there is an invertible matrix P over K such that $B = PAP^{-1}$.*

Recall from Theorem 36.3 that the sequence of $K[X]$-linear maps

$$\begin{tikzcd} 0 \arrow[r] & E[X] \arrow[r, "\psi"] & E[X] \arrow[r, "\sigma"] & E_f \arrow[r] & 0 \end{tikzcd}$$

is exact, and as a consequence, E_f is isomorphic to the quotient of $E[X]$ by $\mathrm{Im}(X1 - \overline{f})$. Furthermore, because E is a vector space, $E[X]$ is a free module with basis $(1 \otimes u_1, \ldots, 1 \otimes u_n)$, where $(u_1, \ldots, u_n)$ is a basis of E, and since ψ is injective, the module $\mathrm{Im}(X1 - \overline{f})$ has rank n. By Theorem 35.31, we have an isomorphism

$$E_f \approx K[X]/(q_1 K[X]) \oplus \cdots \oplus K[X]/(q_n K[X]),$$

and by Proposition 35.32, $E[X]/\mathrm{Im}(X1 - \overline{f})$ is isomorphic to a direct sum

$$E[X]/\mathrm{Im}(X1 - \overline{f}) \approx K[X]/(p_1 K[X]) \oplus \cdots \oplus K[X]/(p_n K[X]),$$

where $p_1, \ldots, p_n$ are the invariant factors of $\mathrm{Im}(X1 - \overline{f})$ with respect to $E[X]$. Since $E_f \approx E[X]/\mathrm{Im}(X1 - \overline{f})$, by the uniqueness part of Theorem 35.31 and because the polynomials are monic, we must have $p_i = q_i$, for $i = 1, \ldots, n$. Therefore, we proved the following crucial fact:

Proposition 36.11. *For any linear map $f\colon E \to E$ over a K-vector space E of dimension n, the similarity invariants of f are equal to the invariant factors of $\mathrm{Im}(X1 - \overline{f})$ with respect to $E[X]$.*

Proposition 36.11 is the key to computing the similarity invariants of a linear map. This can be done using a procedure to convert $XI - M$ to its *Smith normal form.* Propositions 36.11 and 35.37 yield the following result.

Proposition 36.12. *For any linear map $f\colon E \to E$ over a K-vector space E of dimension n, if $(q_1, \ldots, q_n)$ are the similarity invariants of f, for any matrix M representing f with respect to any basis, then for $k = 1, \ldots, n$ the product*

$$d_k(X) = q_1(X) \cdots q_k(X)$$

is the gcd of the $k \times k$-minors of the matrix $XI - M$.

Note that the matrix $XI - M$ is none other than the matrix that yields the characteristic polynomial $\chi_f(X) = \det(XI - M)$ of f.

Proposition 36.13. *For any linear map $f\colon E \to E$ over a K-vector space E of dimension n, if $(q_1, \ldots, q_n)$ are the similarity invariants of f, then the following properties hold:*

(1) If $\chi_f(X)$ is the characteristic polynomial of f, then

$$\chi_f(X) = q_1(X) \cdots q_n(X).$$

(2) The minimal polynomial $m(X) = q_n(X)$ of f divides the characteristic polynomial $\chi_f(X)$ of f.

(3) The characteristic polynomial $\chi_f(X)$ divides $m(X)^n$.

(4) E is cyclic for f iff $m(X) = \chi_f(X)$.

Proof. Property (1) follows from Proposition 36.12 for $k = n$. It also follows from Theorem 36.6 and the fact that for the companion matrix associated with q_i, the characteristic polynomial of this matrix is also q_i. Property (2) is obvious from (1). Since each q_i divides q_{i+1}, each q_i divides q_n, so their product $\chi_f(X)$ divides $m(X)^n = q_n(X)^n$. The last condition says that $q_1 = \cdots = q_{n-1} = 1$, which means that E_f has a single summand. □

Observe that Proposition 36.13 yields another proof of the Cayley–Hamilton Theorem. It also implies that a linear map is nilpotent iff its characteristic polynomial is X^n.

36.3 The Rational Canonical Form, Second Version

Let us now translate the Elementary Divisors Decomposition Theorem, Theorem 35.38, in terms of E_f. We obtain the following result.

Theorem 36.14. *(Cyclic Decomposition Theorem, Second Version) Let $f\colon E \to E$ be an endomorphism on a K-vector space of dimension n. Then, E is the direct sum of of cyclic subspaces $E_j = Z(u_j; f)$ for f, such that the minimal polynomial of E_j is of the form $p_i^{n_{i,j}}$, for some irreducible monic polynomials $p_1, \ldots, p_t \in K[X]$ and some positive integers $n_{i,j}$, such that for each $i = 1, \ldots, t$, there is a sequence of integers*

$$1 \leq \underbrace{n_{i,1}, \ldots, n_{i,1}}_{m_{i,1}} < \underbrace{n_{i,2}, \ldots, n_{i,2}}_{m_{i,2}} < \cdots < \underbrace{n_{i,s_i}, \ldots, n_{i,s_i}}_{m_{i,s_i}},$$

with $s_i \geq 1$, and where $n_{i,j}$ occurs $m_{i,j} \geq 1$ times, for $j = 1, \ldots, s_i$. Furthermore, the monic polynomials p_i and the integers $r, t, n_{i,j}, s_i, m_{i,j}$ are uniquely determined.

Note that there are $\mu = \sum m_{i,j}$ cyclic subspaces $Z(u_j; f)$. Using bases for the cyclic subspaces $Z(u_j; f)$ as in Theorem 36.6, we get the following theorem.

Theorem 36.15. *(Rational Canonical Form, Second Version) Let $f\colon E \to E$ be an endomorphism on a K-vector space of dimension n. There exist t distinct irreducible monic polynomials $p_1, \ldots, p_t \in K[X]$ and some positive integers $n_{i,j}$, such that for each $i = 1, \ldots, t$, there is a sequence of integers*

$$1 \leq \underbrace{n_{i,1}, \ldots, n_{i,1}}_{m_{i,1}} < \underbrace{n_{i,2}, \ldots, n_{i,2}}_{m_{i,2}} < \cdots < \underbrace{n_{i,s_i}, \ldots, n_{i,s_i}}_{m_{i,s_i}},$$

with $s_i \geq 1$, and where $n_{i,j}$ occurs $m_{i,j} \geq 1$ times, for $j = 1, \ldots, s_i$, and there is a basis of E such that the matrix M of f is a block matrix of the form

$$M = \begin{pmatrix} M_1 & 0 & \cdots & 0 & 0 \\ 0 & M_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & M_{\mu-1} & 0 \\ 0 & 0 & \cdots & 0 & M_\mu \end{pmatrix},$$

where each M_j is the companion matrix of some $p_i^{n_{i,j}}$, and $\mu = \sum m_{i,j}$. The monic polynomials $p_1, \ldots, p_t$ and the integers $r, t, n_{i,j}, s_i, m_{i,j}$ are uniquely determined

The polynomials $p_i^{n_{i,j}}$ are called the *elementary divisors* of f (and M). These polynomials are factors of the minimal polynomial.

Example 1 continued: Recall that $f(x, y, z, w) = (x + w, y + z, y + z, x + w)$ has two nontrivial invariant factors $q_1 = x(x - 2) = q_2$. Thus the elementary factors of f are $p_1 = x = p_2$ and $p_3 = x - 2 = p_4$. Theorem 36.14 implies that

$$\mathbb{R}^4 = E_1 \oplus E_2 \oplus E_3 \oplus E_4,$$

where $E_1 = Z(u_1, f) \cong \mathbb{R}[X]/(X)$, $E_2 = Z(u_2, f) \cong \mathbb{R}[X]/(X)$, $E_3 = Z(u_3, f) \cong \mathbb{R}[X]/(X - 2)$, and $E_4 = Z(u_4, f) \cong \mathbb{R}[X]/(X - 2)$. The subspaces E_1 and E_2 correspond to one-dimensional spaces spanned by eigenvectors associated with eigenvalue 0, while E_3 and E_4 correspond to one-dimensional spaces spanned by eigenvectors associated with eigenvalue 2. If we let $u_1 = (-1, 0, 0, 1)$, $u_2 = (0, -1, 1, 0)$, $u_3 = (1, 0, 0, 1)$ and $u_4 = (0, 1, 1, 0)$, Theorem 36.15 gives

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix},$$

as the rational canonical form associated with the cyclic decomposition $\mathbb{R}^4 = E_1 \oplus E_2 \oplus E_3 \oplus E_4$.

As we pointed earlier, unlike the similarity invariants, the elementary divisors may change when we pass to a field extension.

We will now consider the special case where all the irreducible polynomials p_i are of the form $X - \lambda_i$; that is, when are the eigenvalues of f belong to K. In this case, we find again the Jordan form.

36.4 The Jordan Form Revisited

In this section, we assume that all the roots of the minimal polynomial of f belong to K. This will be the case if K is algebraically closed. The irreducible polynomials p_i of Theorem 36.14 are the polynomials $X - \lambda_i$, for the distinct eigenvalues λ_i of f. Then, each cyclic subspace $Z(u_j; f)$ has a minimal polynomial of the form $(X - \lambda)^m$, for some eigenvalue λ of f and some $m \geq 1$. It turns out that by choosing a suitable basis for the cyclic subspace $Z(u_j; f)$, the matrix of the restriction of f to $Z(u_j; f)$ is a Jordan block.

Proposition 36.16. *Let E be a finite-dimensional K-vector space and let $f \colon E \to E$ be a linear map. If E is a cyclic $K[X]$-module and if $(X - \lambda)^n$ is the minimal polynomial of f, then there is a basis of E of the form*

$$((f - \lambda \mathrm{id})^{n-1}(u), (f - \lambda \mathrm{id})^{n-2}(u), \ldots, (f - \lambda \mathrm{id})(u), u),$$

for some $u \in E$. With respect to this basis, the matrix of f is the Jordan block

$$J_n(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & 1 \\ 0 & 0 & 0 & \cdots & \lambda \end{pmatrix}.$$

Proof. Since E is a cyclic $K[X]$-module, there is some $u \in E$ so that E is generated by $u, f(u), f^2(u), \ldots$, which means that every vector in E is of the form $p(f)(u)$, for some polynomial, $p(X)$. We claim that $u, f(u), \ldots, f^{n-2}(u), f^{n-1}(u)$ generate E, which implies that the dimension of E is at most n.

This is because if $p(X)$ is any polynomial of degree at least n, then we can divide $p(X)$ by $(X - \lambda)^n$, obtaining

$$p = (X - \lambda)^n q + r,$$

where $0 \leq \deg(r) < n$, and as $(X - \lambda)^n$ annihilates E, we get

$$p(f)(u) = r(f)(u),$$

which means that every vector of the form $p(f)(u)$ with $p(X)$ of degree $\geq n$ is actually a linear combination of $u, f(u), \ldots, f^{n-2}(u), f^{n-1}(u)$.

We claim that the vectors

$$u, (f - \lambda \mathrm{id})(u), \ldots, (f - \lambda \mathrm{id})^{n-2}(u)(f - \lambda \mathrm{id})^{n-1}(u)$$

are linearly independent. Indeed, if we had a nontrivial linear combination

$$a_0(f - \lambda \mathrm{id})^{n-1}(u) + a_1(f - \lambda \mathrm{id})^{n-2}(u) + \cdots + a_{n-2}(f - \lambda \mathrm{id})(u) + a_{n-1}u = 0,$$

then the polynomial

$$a_0(X - \lambda)^{n-1} + a_1(X - \lambda)^{n-2} + \cdots + a_{n-2}(X - \lambda) + a_{n-1}$$

of degree at most $n - 1$ would annihilate E, contradicting the fact that $(X - \lambda)^n$ is the minimal polynomial of f (and thus, of smallest degree). Consequently, as the dimension of E is at most n,

$$((f - \lambda \mathrm{id})^{n-1}(u), (f - \lambda \mathrm{id})^{n-2}(u), \ldots, (f - \lambda \mathrm{id})(u), u),$$

is a basis of E and since $u, f(u), \ldots, f^{n-2}(u), f^{n-1}(u)$ span E,

$$(u, f(u), \ldots, f^{n-2}(u), f^{n-1}(u))$$

is also a basis of E.

Let us see how f acts on the basis

$$((f - \lambda \mathrm{id})^{n-1}(u), (f - \lambda \mathrm{id})^{n-2}(u), \ldots, (f - \lambda \mathrm{id})(u), u).$$

If we write $f = f - \lambda \mathrm{id} + \lambda \mathrm{id}$, as $(f - \lambda \mathrm{id})^n$ annihilates E, we get

$$f((f - \lambda \mathrm{id})^{n-1}(u)) = (f - \lambda \mathrm{id})^n(u) + \lambda(f - \lambda \mathrm{id})^{n-1}(u) = \lambda(f - \lambda \mathrm{id})^{n-1}(u)$$

and

$$f((f - \lambda \mathrm{id})^k(u)) = (f - \lambda \mathrm{id})^{k+1}(u) + \lambda(f - \lambda \mathrm{id})^k(u), \qquad 0 \leq k \leq n - 2.$$

But this means precisely that the matrix of f in this basis is the Jordan block $J_n(\lambda)$. $\square$

The basis

$$((f-\lambda\mathrm{id})^{n-1}(u),(f-\lambda\mathrm{id})^{n-2}(u),\ldots,(f-\lambda\mathrm{id})(u),u),$$

provided by Proposition 36.16 is known as a *Jordan chain.* Note that $(f-\lambda\mathrm{id})^{n-1}(u)$ is an eigenvector for f. To construct the Jordan chain, we must find u which is a generalized eigenvector of f. This is done by first finding an eigenvector x_1 of f and recursively solving the system $(f-\lambda\mathrm{id})x_{i+1}=x_i$ for $i\leq 1\leq n-1$. For example suppose $f\colon\mathbb{R}^3\to\mathbb{R}^3$ where $f(x,y,z)=(x+y+z,y+z,z)$. In terms of the standard basis, the matrix representation for f is $M=\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}$. By using M, it is readily verified that the minimal polynomial f equals the characteristic polynomial, namely $(X-1)^3$. Thus f has the eigenvalue $\lambda=1$ with repeated three times. To find the eigenvector x_1 associated with $\lambda=1$, we solve the system $(M-I)x_1=0$, or equivalently

$$\begin{pmatrix}0&1&1\\0&0&1\\0&0&0\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}0\\0\\0\end{pmatrix}.$$

Thus $y=z=0$ with $x=1$ solves this system to provide the eigenvector $x_1=\begin{pmatrix}1\\0\\0\end{pmatrix}$. We next solve the system $(M-I)x_2=x_1$, namely

$$\begin{pmatrix}0&1&1\\0&0&1\\0&0&0\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}1\\0\\0\end{pmatrix},$$

which implies that $z=0$ and $y=1$. Hence $x_2=\begin{pmatrix}1\\1\\0\end{pmatrix}$ will work. To finish constructing our Jordan chain, we must solve the system $(M-I)x_3=x_2$, namely

$$\begin{pmatrix}0&1&1\\0&0&1\\0&0&0\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}1\\1\\0\end{pmatrix},$$

from which we see that $z=1$, $y=0$, and $x_3=\begin{pmatrix}1\\0\\1\end{pmatrix}$. By setting $x_3=u$, we form the basis

$$((f-\lambda\mathrm{id})^2(u),(f-\lambda\mathrm{id})^1(u),\ldots,(f-\lambda\mathrm{id})(u),u)=(x_1,x_2,x_3).$$

In terms of the basis (x_1, x_2, x_3), the map $f(x, y, z) = (x + y + z, y + z, z)$ has the Jordan block matrix representation $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ since

$$\begin{aligned} f(x_1) &= f(1, 0, 0) = (1, 0, 0) = x_1 \\ f(x_2) &= f(1, 1, 0) = (2, 1, 0) = x_1 + x_2 \\ f(x_3) &= f(1, 0, 1) = (2, 1, 1) = x_2 + x_3. \end{aligned}$$

Combining Theorem 36.15 and Proposition 36.16, we obtain a strong version of the Jordan form.

Theorem 36.17. *(Jordan Canonical Form) Let E be finite-dimensional K-vector space. The following properties are equivalent:*

(1) The eigenvalues of f all belong to K.

(2) There is a basis of E in which the matrix of f is upper (or lower) triangular.

(3) There exist a basis of E in which the matrix A of f is Jordan matrix. Furthermore, the number of Jordan blocks $J_r(\lambda)$ appearing in A, for fixed r and λ, is uniquely determined by f.

Proof. The implication (1) $\Longrightarrow$ (3) follows from Theorem 36.15 and Proposition 36.16. The implications (3) $\Longrightarrow$ (2) and (2) $\Longrightarrow$ (1) are trivial. □

Compared to Theorem 31.17, the new ingredient is the uniqueness assertion in (3), which is not so easy to prove.

Observe that the minimal polynomial of f is the least common multiple of the polynomials $(X - \lambda)^r$ associated with the Jordan blocks $J_r(\lambda)$ appearing in A, and the characteristic polynomial of A is the product of these polynomials.

We now return to the problem of computing effectively the similarity invariants of a matrix M. By Proposition 36.11, this is equivalent to computing the invariant factors of $XI - M$. In principle, this can be done using Proposition 35.35. A procedure to do this effectively for the ring $A = K[X]$ is to convert $XI - M$ to its Smith normal form. This will also yield the rational canonical form for M.

36.5 The Smith Normal Form

The Smith normal form is the special case of Proposition 35.35 applied to the PID $K[X]$ where K is a field, but it also says that the matrices P and Q are products of elementary matrices. It turns out that such a result holds for any Euclidean ring, and the proof is basically the same.

Recall from Definition 30.10 that a *Euclidean ring* is an integral domain A such that there exists a function $\sigma\colon A \to \mathbb{N}$ with the following property: For all $a, b \in A$ with $b \neq 0$, there are some $q, r \in A$ such that

$$a = bq + r \quad \text{and} \quad \sigma(r) < \sigma(b).$$

Note that the pair (q, r) is not necessarily unique.

We make use of the elementary row and column operations $P(i,k)$, $E_{i,j;\beta}$, and $E_{i,\lambda}$ described in Chapter 8, where we require the scalar λ used in $E_{i,\lambda}$ to be a unit.

Theorem 36.18. *If M is an $m \times n$ matrix over a Euclidean ring A, then there exist some invertible $n \times n$ matrix P and some invertible $m \times m$ matrix Q, where P and Q are products of elementary matrices, and a $m \times n$ matrix D of the form*

$$D = \begin{pmatrix} \alpha_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \alpha_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & \alpha_r & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

for some nonzero $\alpha_i \in A$, such that

(1) $\alpha_1 \mid \alpha_2 \mid \cdots \mid \alpha_r$, and

(2) $M = QDP^{-1}$.

Proof. We follow Jacobson's proof [97] (Chapter 3, Theorem 3.8). We proceed by induction on $m + n$.

If $m = n = 1$, let $P = (1)$ and $Q = (1)$.

For the induction step, if $M = 0$, let $P = I_n$ and $Q = I_m$. If $M \neq 0$, the stategy is to apply a sequence of elementary transformations that converts M to a matrix of the form

$$M' = \begin{pmatrix} \alpha_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & Y & \\ 0 & & & \end{pmatrix}$$

where Y is a $(m-1) \times (n-1)$-matrix such that α_1 divides every entry in Y. Then, we proceed by induction on Y. To find M', we perform the following steps.

Step 1. Pick some nonzero entry a_{ij} in M such that $\sigma(a_{ij})$ is minimal. Then permute column j and column 1, and permute row i and row 1, to bring this entry in position $(1,1)$. We denote this new matrix again by M.

Step 2a.

If $m = 1$ go to Step 2b.

If $m > 1$, then there are two possibilities:

(i) M is of the form

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{m2} & \cdots & a_{mn} \end{pmatrix}.$$

If $n = 1$, stop; else go to Step 2b.

(ii) There is some nonzero entry a_{i1} $(i > 1)$ below a_{11} in the first column.

(a) If there is some entry a_{k1} in the first column such that a_{11} does not divide a_{k1}, then pick such an entry (say, with the smallest index i such that $\sigma(a_{i1})$ is minimal), and divide a_{k1} by a_{11}; that is, find b_k and b_{k1} such that

$$a_{k1} = a_{11}b_k + b_{k1}, \quad \text{with} \quad \sigma(b_{k1}) < \sigma(a_{11}).$$

Subtract b_k times row 1 from row k and permute row k and row 1, to obtain a matrix of the form

$$M = \begin{pmatrix} b_{k1} & b_{k2} & \cdots & b_{kn} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}.$$

Go back to Step 2a.

(b) If a_{11} divides every (nonzero) entry a_{i1} for $i \geq 2$, say $a_{i1} = a_{11}b_i$, then subtract b_i times row 1 from row i for $i = 2, \ldots, m$; go to Step 2b.

Observe that whenever we return to the beginning of Step 2a, we have $\sigma(b_{k1}) < \sigma(a_{11})$. Therefore, after a finite number of steps, we must exit Step 2a with a matrix in which all entries in column 1 but the first are zero and go to Step 2b.

Step 2b.

This step is reached only if $n > 1$ and if the only nonzero entry in the first column is a_{11}.

(a) If M is of the form

$$\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

and $m = 1$ stop; else go to Step 3.

(b) If there is some entry a_{1k} in the first row such that a_{11} does not divide a_{1k}, then pick such an entry (say, with the smallest index j such that $\sigma(a_{1j})$ is minimal), and divide a_{1k} by a_{11}; that is, find b_k and b_{1k} such that

$$a_{1k} = a_{11}b_k + b_{1k}, \quad \text{with} \quad \sigma(b_{1k}) < \sigma(a_{11}).$$

Subtract b_k times column 1 from column k and permute column k and column 1, to obtain a matrix of the form

$$M = \begin{pmatrix} b_{1k} & a_{k2} & \cdots & a_{kn} \\ b_{2k} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{mk} & a_{m2} & \cdots & a_{mn} \end{pmatrix}.$$

Go back to Step 2b.

(c) If a_{11} divides every (nonzero) entry a_{1j} for $j \geq 2$, say $a_{1j} = a_{11}b_j$, then subtract b_j times column 1 from column j for $j = 2, \ldots, n$; go to Step 3.

As in Step 2a, whenever we return to the beginning of Step 2b, we have $\sigma(b_{1k}) < \sigma(a_{11})$. Therefore, after a finite number of steps, we must exit Step 2b with a matrix in which all entries in row 1 but the first are zero.

Step 3. This step is reached only if the only nonzero entry in the first row is a_{11}.

(i) If

$$M = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & Y & \\ 0 & & & \end{pmatrix}$$

go to Step 4.

(ii) If Step 2b ruined column 1 which now contains some nonzero entry below a_{11}, go back to Step 2a.

We perform a sequence of alternating steps between Step 2a and Step 2b. Because the σ-value of the $(1, 1)$-entry strictly decreases whenever we reenter Step 2a and Step 2b, such a sequence must terminate with a matrix of the form

$$M = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & Y & \\ 0 & & & \end{pmatrix}$$

Step 4. If a_{11} divides all entries in Y, stop.

Otherwise, there is some column, say j, such that a_{11} does not divide some entry a_{ij}, so add the jth column to the first column. This yields a matrix of the form

$$M = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ b_{2j} & & & \\ \vdots & & Y & \\ b_{mj} & & & \end{pmatrix}$$

where the ith entry in column 1 is nonzero, so go back to Step 2a,

Again, since the σ-value of the $(1,1)$-entry strictly decreases whenever we reenter Step 2a and Step 2b, such a sequence must terminate with a matrix of the form

$$M' = \begin{pmatrix} \alpha_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & Y & \\ 0 & & & \end{pmatrix}$$

where α_1 divides every entry in Y. Then, we apply the induction hypothesis to Y. □

If the PID A is the polynomial ring $K[X]$ where K is a field, the α_i are nonzero polynomials, so we can apply row operations to normalize their leading coefficients to be 1. We obtain the following theorem.

Theorem 36.19. *(Smith Normal Form) If M is an $m \times n$ matrix over the polynomial ring $K[X]$, where K is a field, then there exist some invertible $n \times n$ matrix P and some invertible $m \times m$ matrix Q, where P and Q are products of elementary matrices with entries in $K[X]$, and a $m \times n$ matrix D of the form*

$$D = \begin{pmatrix} q_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & q_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & q_r & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

for some nonzero monic polynomials $q_i \in k[X]$, such that

(1) $q_1 \mid q_2 \mid \cdots \mid q_r$, and

(2) $M = QDP^{-1}$.

In particular, if we apply Theorem 36.19 to a matrix M of the form $M = XI - A$, where A is a square matrix, then $\det(XI - A) = \chi_A(X)$ is never zero, and since $XI - A = QDP^{-1}$ with P, Q invertible, all the entries in D must be nonzero and we obtain the following result showing that the similarity invariants of A can be computed using elementary operations.

Theorem 36.20. *If A is an $n \times n$ matrix over the field K, then there exist some invertible $n \times n$ matrices P and Q, where P and Q are products of elementary matrices with entries in $K[X]$, and a $n \times n$ matrix D of the form*

$$D = \begin{pmatrix} 1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & q_1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & q_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & q_m \end{pmatrix}$$

for some nonzero monic polynomials $q_i \in k[X]$ of degree ≥ 1, such that

(1) $q_1 \mid q_2 \mid \cdots \mid q_m$,

(2) $q_1, \ldots q_m$ are the similarity invariants of A, and

(3) $XI - A = QDP^{-1}$.

The matrix D in Theorem 36.20 is often called *Smith normal form* of A, even though this is confusing terminology since D is really the Smith normal form of $XI - A$.

Of course, we know from previous work that in Theorem 36.19, the $\alpha_1, \ldots, \alpha_r$ are unique, and that in Theorem 36.20, the $q_1, \ldots, q_m$ are unique. This can also be proved using some simple properties of minors, but we leave it as an exercise (for help, look at Jacobson [97], Chapter 3, Theorem 3.9).

The rational canonical form of A can also be obtained from Q^{-1} and D, but first, let us consider the generalization of Theorem 36.19 to PID's that are not necessarily Euclidean rings.

We need to find a "norm" that assigns a natural number $\sigma(a)$ to any nonzero element of a PID A, in such a way that $\sigma(a)$ decreases whenever we return to Step 2a and Step 2b. Since a PID is a UFD, we use the number

$$\sigma(a) = k_1 + \cdots + k_r$$

of prime factors in the factorization of a nonunit element

$$a = up_1^{k_1} \cdots p_r^{k_r},$$

and we set

$$\sigma(u) = 0$$

if u is a unit.

We can't divide anymore, but we can find gcd's and use Bezout to mimic division. The key ingredient is this: for any two nonzero elements $a, b \in A$, if a does not divide b then let $d \neq 0$ be a gcd of a and b. By Bezout, there exist $x, y \in A$ such that

$$ax + by = d.$$

We can also write $a = td$ and $b = -sd$, for some $s, t \in A$, so that $tdx - sdy = d$, which implies that

$$tx - sy = 1,$$

since A is an integral domain. Observe that

$$\begin{pmatrix} t & -s \\ -y & x \end{pmatrix} \begin{pmatrix} x & s \\ y & t \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

which shows that both matrices on the left of the equation are invertible, and so is the transpose of the second one,

$$\begin{pmatrix} x & y \\ s & t \end{pmatrix}$$

(they all have determinant 1). We also have

$$as + bt = tds - sdt = 0,$$

so

$$\begin{pmatrix} x & y \\ s & t \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}$$

and

$$\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} x & s \\ y & t \end{pmatrix} = \begin{pmatrix} d & 0 \end{pmatrix}.$$

Because a does not divide b, their gcd d has strictly fewer prime factors than a, so

$$\sigma(d) < \sigma(a).$$

Using matrices of the form

$$\begin{pmatrix} x & y & 0 & 0 & \cdots & 0 \\ s & t & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix}$$

with $xt - ys = 1$, we can modify Steps 2a and Step 2b to obtain the following theorem.

Theorem 36.21. *If M is an $m \times n$ matrix over a PID A, then there exist some invertible $n \times n$ matrix P and some invertible $m \times m$ matrix Q, where P and Q are products of elementary matrices and matrices of the form*

$$\begin{pmatrix} x & y & 0 & 0 & \cdots & 0 \\ s & t & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix}$$

with $xt - ys = 1$, and a $m \times n$ matrix D of the form

$$D = \begin{pmatrix} \alpha_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \alpha_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & \alpha_r & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

for some nonzero $\alpha_i \in A$, such that

(1) $\alpha_1 \mid \alpha_2 \mid \cdots \mid \alpha_r$, and

(2) $M = QDP^{-1}$.

Proof sketch. In Step 2a, if a_{11} does not divide a_{k1}, then first permute row 2 and row k (if $k \neq 2$). Then, if we write $a = a_{11}$ and $b = a_{k1}$, if d is a gcd of a and b and if x, y, s, t are determined as explained above, multiply on the left by the matrix

$$\begin{pmatrix} x & y & 0 & 0 & \cdots & 0 \\ s & t & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix}$$

to obtain a matrix of the form

$$\begin{pmatrix} d & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ a_{31} & a_{32} & \cdots & a_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}$$

with $\sigma(d) < \sigma(a_{11})$. Then, go back to Step 2a.

In Step 2b, if a_{11} does not divide a_{1k}, then first permute column 2 and column k (if $k \neq 2$). Then, if we write $a = a_{11}$ and $b = a_{1k}$, if d is a gcd of a and b and if x, y, s, t are determined as explained above, multiply on the right by the matrix

$$\begin{pmatrix} x & s & 0 & 0 & \cdots & 0 \\ y & t & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix}$$

to obtain a matrix of the form

$$\begin{pmatrix} d & 0 & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \ldots & a_{mn} \end{pmatrix}$$

with $\sigma(d) < \sigma(a_{11})$. Then, go back to Step 2b. The other steps remain the same. Whenever we return to Step 2a or Step 2b, the σ-value of the $(1,1)$-entry strictly decreases, so the whole procedure terminates. □

We conclude this section by explaining how the rational canonical form of a matrix A can be obtained from the canonical form QDP^{-1} of $XI - A$.

Let $f \colon E \to E$ be a linear map over a K-vector space of dimension n. Recall from Theorem 36.3 (see Section 36.1) that as a $K[X]$-module, E_f is the image of the free module $E[X]$ by the map $\sigma \colon E[X] \to E_f$, where $E[X]$ consists of all linear combinations of the form

$$p_1 e_1 + \cdots + p_n e_n,$$

where $(e_1, \ldots, e_n)$ is a basis of E and $p_1, \ldots, p_n \in K[X]$ are polynomials, and σ is given by

$$\sigma(p_1 e_1 + \cdots + p_n e_n) = p_1(f)(e_1) + \cdots + p_n(f)(e_n).$$

Furthermore, the kernel of σ is equal to the image of the map $\psi \colon E[X] \to E[X]$, where

$$\psi(p_1 e_1 + \cdots + p_n e_n) = Xp_1 e_1 + \cdots + Xp_n e_n - (p_1 f(e_1) + \cdots + p_n(e_n)).$$

The matrix A is the representation of a linear map f over the canonical basis $(e_1, \ldots, e_n)$ of $E = K^n$, and and $XI - A$ is the matrix of ψ with respect to the basis $(e_1, \ldots, e_n)$

(over $K[X]$). What Theorem 36.20 tells us is that there are $K[X]$-bases $(u_1, \ldots, u_n)$ and $(v_1, \ldots, v_n)$ of E_f with respect to which the matrix of ψ is D. Then

$$\begin{aligned} \psi(u_i) &= v_i, \quad i = 1, \ldots, n-m, \\ \psi(u_{n-m+i}) &= q_i v_{n-m+i}, \quad i = 1, \ldots, m, \end{aligned}$$

and because $\mathrm{Im}(\psi) = \mathrm{Ker}\,(\sigma)$, this implies that

$$\sigma(v_i) = 0, \quad i = 1, \ldots, n-m.$$

Consequently, $w_1 = \sigma(v_{n-m+1}), \ldots, w_m = \sigma(v_n)$ span E_f as a $K[X]$-module, with $w_i \in E$, and we have

$$M(f) = K[X]w_1 \oplus \cdots \oplus K[X]w_m,$$

where $K[X]w_i \approx K[X]/(q_i)$ as a cyclic $K[X]$-module. Since $\mathrm{Im}(\psi) = \mathrm{Ker}\,(\sigma)$, we have

$$0 = \sigma(\psi(u_{n-m+i})) = \sigma(q_i v_{n-m+i}) = q_i \sigma(v_{n-m+i}) = q_i w_i,$$

so as a K-vector space, the cyclic subspace $Z(w_i; f) = K[X]w_i$ has q_i as annihilator, and by a remark from Section 36.1, it has the basis (over K)

$$(w_i, f(w_i), \ldots, f^{n_i - 1}(w_i)), \quad n_i = \deg(q_i).$$

Furthermore, over this basis, the restriction of f to $Z(w_i; f)$ is represented by the companion matrix of q_i. By putting all these bases together, we obtain a block matrix which is the canonical rational form of f (and A).

Now, $XI - A = QDP^{-1}$ is the matrix of ψ with respect to the canonical basis $(e_1, \ldots, e_n)$ (over $K[X]$), and D is the matrix of ψ with respect to the bases $(u_1, \ldots, u_n)$ and $(v_1, \ldots, v_n)$ (over $K[X]$), which tells us that the columns of Q consist of the coordinates (in $K[X]$) of the basis vectors $(v_1, \ldots, v_n)$ with respect to the basis $(e_1, \ldots, e_n)$. Therefore, the coordinates (in K) of the vectors $(w_1, \ldots, w_m)$ spanning E_f over $K[X]$, where $w_i = \sigma(v_{n-m+i})$, are obtained by substituting the matrix A for X in the coordinates of the columns vectors of Q, and evaluating the resulting expressions.

Since

$$D = Q^{-1}(XI - A)P,$$

the matrix D is obtained from A by a sequence of elementary row operations whose product is Q^{-1} and a sequence of elementary column operations whose product is P. Therefore, to compute the vectors $w_1, \ldots, w_m$ from A, we simply have to figure out how to construct Q from the sequence of elementary row operations that yield Q^{-1}. The trick is to use column operations to gather a product of row operations in reverse order.

Indeed, if Q^{-1} is the product of elementary row operations

$$Q^{-1} = E_k \cdots E_2 E_1,$$

then

$$Q = E_1^{-1} E_2^{-1} \cdots E_k^{-1}.$$

Now, row operations operate on the left and column operations operate on the right, so the product $E_1^{-1} E_2^{-1} \cdots E_k^{-1}$ can be computed from left to right as a sequence of column operations.

Let us review the meaning of the elementary row and column operations $P(i, k)$, $E_{i,j;\beta}$, and $E_{i,\lambda}$.

1. As a row operation, $P(i, k)$ permutes row i and row k.
2. As a column operation, $P(i, k)$ permutes column i and column k.
3. The inverse of $P(i, k)$ is $P(i, k)$ itself.
4. As a row operation, $E_{i,j;\beta}$ adds β times row j to row i.
5. As a column operation, $E_{i,j;\beta}$ adds β times column i to column j (note the switch in the indices).
6. The inverse of $E_{i,j;\beta}$ is $E_{i,j;-\beta}$.
7. As a row operation, $E_{i,\lambda}$ multiplies row i by λ.
8. As a column operation, $E_{i,\lambda}$ multiplies column i by λ.
9. The inverse of $E_{i,\lambda}$ is $E_{i,\lambda^{-1}}$.

Given a square matrix A (over K), the row and column operations applied to $XI - A$ in converting it to its Smith normal form may involve coefficients that are polynomials and it is necessary to explain what is the action of an operation $E_{i,j;\beta}$ in this case. If the coefficient β in $E_{i,j;\beta}$ is a polynomial over K, as a row operation, the action of $E_{i,j;\beta}$ on a matrix X is to multiply the jth row of M by the matrix $\beta(A)$ obtained by substituting the matrix A for X and then to add the resulting vector to row i. Similarly, as a column operation, the action of $E_{i,j;\beta}$ on a matrix X is to multiply the ith column of M by the matrix $\beta(A)$ obtained by substituting the matrix A for X and then to add the resulting vector to column j. An algorithm to compute the rational canonical form of a matrix can now be given. We apply the elementary column operations E_i^{-1} for $i = 1, \ldots k$, starting with the identity matrix.

Algorithm for Converting an $n \times n$ matrix to Rational Canonical Form

While applying elementary row and column operations to compute the Smith normal form D of $XI - A$, keep track of the row operations and perform the following steps:

1. Let $P' = I_n$, and for every elementary row operation E do the following:
   (a) If $E = P(i, k)$, permute column i and column k of P'.

(b) If $E = E_{i,j;\beta}$, multiply the ith column of P' by the matrix $\beta(A)$ obtained by substituting the matrix A for X, and then subtract the resulting vector from column j.

(c) If $E = E_{i,\lambda}$ where $\lambda \in K$, then multiply the ith column of P' by λ^{-1}.

2. When step (1) terminates, the first $n - m$ columns of P' are zero and the last m are linearly independent. For $i = 1, \ldots, m$, multiply the $(n - m + i)$th column w_i of P' successively by $I, A^1, A^2, A^{n_i - 1}$, where n_i is the degree of the polynomial q_i (appearing in D), and form the $n \times n$ matrix P consisting of the vectors
$$w_1, Aw_1, \ldots, A^{n_1-1}w_1, w_2, Aw_2, \ldots, A^{n_2-1}w_2, \ldots, w_m, Aw_m, \ldots, A^{n_m-1}w_m.$$
Then, $P^{-1}AP$ is the canonical rational form of A.

Here is an example taken from Dummit and Foote [55] (Chapter 12, Section 12.2). Let A be the matrix
$$A = \begin{pmatrix} 1 & 2 & -4 & 4 \\ 2 & -1 & 4 & -8 \\ 1 & 0 & 1 & -2 \\ 0 & 1 & -2 & 3 \end{pmatrix}.$$
One should check that the following sequence of row and column operations produces the Smith normal form D of $XI - A$:

row $P(1,3)$	row $E_{1,-1}$	row $E_{2,1;2}$	row $E_{3,1;-(X-1)}$	column $E_{1,3;X-1}$	column $E_{1,4;2}$
row $P(2,4)$	row$E_{2,-1}$	row $E_{3,2;2}$	row $E_{4,2;-(X+1)}$	column $E_{2,3;2}$	column $E_{2,4;X-3}$,

with
$$D = \begin{pmatrix} 1 & 0 & 0 & \\ 0 & 1 & 0 & 0 \\ 0 & 0 & (X-1)^2 & 0 \\ 0 & 0 & 0 & (X-1)^2 \end{pmatrix}.$$
Then, applying Step 1 of the above algorithm, we get the sequence of column operations:
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \xrightarrow{P(1,3)} \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \xrightarrow{E_{1,-1}} \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \xrightarrow{E_{2,1,-2}}$$
$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ -2 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \xrightarrow{E_{3,1,A-I}} \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \xrightarrow{P(2,4)} \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \xrightarrow{E_{2,-1}}$$
$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \xrightarrow{E_{3,2,-2}} \begin{pmatrix} 0 & -2 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \xrightarrow{E_{4,2;A+I}} \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = P'.$$

Step 2 of the algorithm yields the vectors

$$\begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \quad A\begin{pmatrix}1\\0\\0\\0\end{pmatrix} = \begin{pmatrix}1\\2\\1\\0\end{pmatrix}, \quad \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \quad A\begin{pmatrix}0\\1\\0\\0\end{pmatrix} = \begin{pmatrix}2\\-1\\0\\1\end{pmatrix},$$

so we get

$$P = \begin{pmatrix}1 & 1 & 0 & 2\\0 & 2 & 1 & -1\\0 & 1 & 0 & 0\\0 & 0 & 0 & 1\end{pmatrix}.$$

We find that

$$P^{-1} = \begin{pmatrix}1 & 0 & -1 & -2\\0 & 0 & 1 & 0\\0 & 1 & -2 & 1\\0 & 0 & 0 & 1\end{pmatrix},$$

and thus, the rational canonical form of A is

$$P^{-1}AP = \begin{pmatrix}0 & -1 & 0 & 0\\1 & 2 & 0 & 0\\0 & 0 & 0 & -1\\0 & 0 & 1 & 2\end{pmatrix}.$$