

# Chapter 1

## $\lambda$ -Rings

The definition of a  $\lambda$ -ring involves certain polynomials that arise in the theory of symmetric functions. We will, therefore, begin by discussing symmetric functions in §1.1. This material is fairly standard and can be found in most books on abstract algebra, e.g., Chapter 2 in [Jacobson (1985)].

The definition of a  $\lambda$ -ring and some of its basic properties are given in §1.2. In §1.3 we discuss the free  $\lambda$ -ring on one generator. This is used in §1.4 to prove the Verification Principle, which states that a natural operation on  $\lambda$ -rings is uniquely determined by its actions on sums of one-dimensional elements. The Splitting Principle is discussed in §1.5. This result allows one to write an  $n$ -dimensional element in a  $\lambda$ -ring as a sum of  $n$  one-dimensional elements. The materials on the free  $\lambda$ -ring, the Verification Principle, and the Splitting Principle originated in the paper [Atiyah and Tall (1969)] by Atiyah and Tall. Another reference is Knutson's book [Knutson (1973)]. The original sources for  $\lambda$ -rings are [Berthelot (1971); Grothendieck (1971)].

Throughout this book, we use the following standard notations:

- $\mathbf{Z}$ , the integers,
- $\mathbf{Z}_{(p)}$ , the  $p$ -local integers for a prime  $p$ ,
- $\mathbf{Q}$ , the rationals,
- $\mathbf{C}$ , the complex numbers.

Unless otherwise specified, by a *ring* we always mean an associative and commutative ring with a multiplicative identity  $1 \neq 0$ . Ring homomorphisms are required to preserve the multiplicative identity. An object  $R$  that satisfies all the ring axioms except for the existence of a multiplicative identity is called a *non-unital ring*. Non-unital rings will be used in §3.3.

### 1.1 Symmetric Functions

Fix a ring  $R$ . Let  $R[x_1, \dots, x_n]$  be the polynomial ring over  $R$  in  $n$  independent variables  $x_1, \dots, x_n$ . If  $f \in R[x_1, \dots, x_n]$  and  $\pi$  is a permutation on  $\{1, \dots, n\}$ , then

$\pi f$  is defined as the polynomial

$$\pi f = f(x_{\pi(1)}, \dots, x_{\pi(n)}).$$

A polynomial  $f \in R[x_1, \dots, x_n]$  is called a *symmetric function* if  $\pi f = f$  for every permutation  $\pi$  on  $\{1, \dots, n\}$ .

**Example 1.1.** For  $1 \leq k \leq n$ , let  $s_k \in R[x_1, \dots, x_n]$  be the polynomial

$$s_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k}.$$

For example, we have

$$\begin{aligned} s_1 &= x_1 + \cdots + x_n, \\ s_2 &= x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n, \\ s_n &= x_1 x_2 \cdots x_n. \end{aligned}$$

Each  $s_k$  is a symmetric function, since  $s_k$  is the coefficient of  $t^{n-k}$  in

$$\begin{aligned} \prod_{k=1}^n (t - x_k) &= (t - x_1)(t - x_2) \cdots (t - x_n) \\ &= t^n - s_1 t^{n-1} + s_2 t^{n-2} - \cdots + (-1)^n s_n. \end{aligned} \tag{1.1}$$

The polynomial  $s_k$  is called the *kth elementary symmetric function on  $x_1, \dots, x_n$* . We will sometimes write  $s_k(x_1, \dots, x_n)$  for  $s_k$  to avoid any ambiguity.

Another way to define the elementary symmetric functions is by looking at their generating function:

$$\prod_{k=1}^n (1 + x_k t) = 1 + s_1 t + s_2 t^2 + \cdots + s_n t^n. \tag{1.2}$$

Note that

$$s_k(x_1, \dots, x_n, 0) = s_k(x_1, \dots, x_n).$$

**Example 1.2.** For any positive integer  $r$ , the  $r$ th power sum

$$x_1^r + \cdots + x_n^r$$

is a symmetric function.

**Example 1.3.** For any positive integers  $m$  and  $n$ , consider the polynomial

$$g(t) = \prod_{1 \leq i_1 < \dots < i_m \leq mn} (1 + x_{i_1} \cdots x_{i_m} t)$$

Then the coefficient of each  $t^j$  in  $g$  is a symmetric function in the variables  $x_1, \dots, x_{mn}$ .

A fundamental property of symmetric functions is that they are all generated by the elementary symmetric functions.

**Theorem 1.4 (The Fundamental Theorem of Symmetric Functions).**

The elementary symmetric functions  $s_1, \dots, s_n$  in  $R[x_1, \dots, x_n]$  are algebraically independent over  $R$ . Moreover, every symmetric function  $f$  in  $R[x_1, \dots, x_n]$  can be written uniquely as a polynomial with coefficients in  $R$  in the elementary symmetric functions.

Before giving the proof, we need the following terminology. The *degree* of a monomial

$$x_1^{k_1} \cdots x_n^{k_n} \tag{1.3}$$

is  $k_1 + \cdots + k_n$ . A polynomial  $f \in R[x_1, \dots, x_n]$  is said to be *homogeneous of degree  $m$*  if every non-zero monomial in  $f$  has degree  $m$ . We order monomials *lexicographically*. In other words, we say that

$$x_1^{k_1} \cdots x_n^{k_n} \text{ is higher than } x_1^{l_1} \cdots x_n^{l_n} \tag{1.4}$$

if there exists  $s \in \{1, \dots, n\}$  such that  $k_i = l_i$  for  $i < s$  and  $k_s > l_s$ .

**Example 1.5.** The elementary symmetric function  $s_k = s_k(x_1, \dots, x_n)$  is homogeneous of degree  $k$ . The highest monomial in  $s_k$  is  $x_1 x_2 \cdots x_k$ . In general, given non-negative integers  $l_1, \dots, l_n$ , the polynomial  $s_1^{l_1} \cdots s_n^{l_n}$  is homogeneous of degree

$$l_1 + 2l_2 + \cdots + nl_n = \sum_{k=1}^n kl_k.$$

Its highest monomial is

$$x_1^{l_1 + \cdots + l_n} x_2^{l_2 + \cdots + l_n} \cdots x_n^{l_n}.$$

Moreover, if  $s_1^{j_1} \cdots s_n^{j_n}$  has the same highest monomial as that of  $s_1^{l_1} \cdots s_n^{l_n}$ , then  $j_n = l_n$  from the exponents of  $x_n$ . Therefore,  $j_{n-1} = l_{n-1}$  from the exponents of  $x_{n-1}$ , and so forth. So  $j_i = l_i$  for  $i = 1, \dots, n$ .

**Proof.** [Proof of Theorem 1.4] First we prove that every symmetric function  $f$  in  $R[x_1, \dots, x_n]$  can be written as a polynomial with coefficients in  $R$  in the elementary symmetric functions. It suffices to prove this when  $f$  is homogenous, say, of degree  $m$ . Suppose that  $x_1^{k_1} \cdots x_n^{k_n}$  is the highest monomial in  $f$  with non-zero coefficient. Since  $f$  is symmetric, it has a monomial of the form  $x_{\pi(1)}^{k_1} \cdots x_{\pi(n)}^{k_n}$  for any permutation  $\pi$ . Since  $x_1^{k_1} \cdots x_n^{k_n}$  is the highest monomial in  $f$ , it follows that  $k_i \geq k_{i+1}$  for  $i = 1, \dots, n-1$ .

From Example 1.5, the polynomial  $s_1^{k_1 - k_2} s_2^{k_2 - k_3} \cdots s_n^{k_n}$  is homogeneous of degree  $k_1 + \cdots + k_n = m$  and has highest monomial  $x_1^{k_1} \cdots x_n^{k_n}$ . If the coefficient of  $x_1^{k_1} \cdots x_n^{k_n}$  in  $f$  is  $r$ , then the polynomial

$$f_1 = f - r s_1^{k_1 - k_2} s_2^{k_2 - k_3} \cdots s_n^{k_n}$$

is homogeneous of degree  $m$ , whose highest monomial is less than  $x_1^{k_1} \cdots x_n^{k_n}$ . Now we apply the same procedure to  $f_1$ , and so forth. The procedure has to stop after a

finite number of steps, since there are only finitely many monomials in  $R[x_1, \dots, x_n]$  of degree  $m$ . This shows that every symmetric function  $f \in R[x_1, \dots, x_n]$  can be written as a polynomial in the elementary symmetric functions.

Next we show that the elementary symmetric functions are algebraically independent over  $R$ . Indeed, if they are not algebraically independent, then there is a non-trivial relation

$$\sum r_{(d_1, \dots, d_n)} s_1^{d_1} \cdots s_n^{d_n} = 0$$

in which every coefficient  $r_{(d_1, \dots, d_n)} \neq 0$  in  $R$ . Among the multi-indexes  $(d_1, \dots, d_n)$ , choose the one for which  $s_1^{d_1} \cdots s_n^{d_n}$  has the highest degree and the highest monomial, say,  $x_1^{k_1} \cdots x_n^{k_n}$ . From Example 1.5 again, this monomial only appears once. This is a contradiction to the algebraic independence of the variables  $x_1, \dots, x_n$ . This proves that the elementary symmetric functions are algebraically independent.

The uniqueness assertion in the Theorem now follows from the algebraic independence of the elementary symmetric functions. □

**Example 1.6.** The square sum can be expressed as

$$x_1^2 + \cdots + x_n^2 = (x_1 + \cdots + x_n)^2 - 2 \left( \sum_{i < j} x_i x_j \right) = s_1^2 - 2s_2.$$

In general, there is a polynomial  $Q_r$  with integer coefficients such that

$$x_1^r + \cdots + x_n^r = Q_r(s_1, \dots, s_n).$$

These polynomials  $Q_r$  will be used in Theorem 3.9 to express Adams operations in terms of  $\lambda$ -operations.

**Example 1.7.** In the polynomial

$$\prod_{1 \leq i < j \leq 4} (1 + x_i x_j t),$$

the coefficient of  $t$  is  $s_2$  and the coefficient of  $t^6$  is  $s_4^3$ . In general, there is a universal polynomial  $P_{n,m}$  in  $nm$  variables with integer coefficients such that the coefficient of  $t^n$  in

$$g(t) = \prod_{1 \leq i_1 < \cdots < i_m \leq nm} (1 + x_{i_1} \cdots x_{i_m} t)$$

is  $P_{n,m}(s_1, \dots, s_{nm})$ . These polynomials  $P_{n,m}$  will appear in the definition of a  $\lambda$ -ring (Definition 1.10).

For example,  $P_{n,1}(s_1, \dots, s_n)$  is the coefficient of  $t^n$  in

$$\prod_{1 \leq i \leq n} (1 + x_i t) = (1 + x_1 t) \cdots (1 + x_n t),$$

which is  $x_1 \cdots x_n = s_n$ . In other words, we have

$$P_{n,1}(s_1, \dots, s_n) = s_n. \tag{1.5}$$

Similarly,  $P_{1,m}(s_1, \dots, s_m)$  is the coefficient of  $t$  in

$$\prod_{1 \leq i_1 < \cdots < i_m \leq m} (1 + x_{i_1} \cdots x_{i_m} t) = 1 + (x_1 \cdots x_m) t.$$

So we have

$$P_{1,m}(s_1, \dots, s_m) = s_m. \tag{1.6}$$

### 1.1.1 Symmetric functions in two sets of variables

We will need a slight generalization of Theorem 1.4. Let  $y_1, \dots, y_n$  be another set of variables, and let  $\sigma_1, \dots, \sigma_n$  be their elementary symmetric functions. Let  $f$  be an element in the polynomial ring  $R[x_1, \dots, x_n; y_1, \dots, y_n]$ . We say that  $f$  is a *symmetric function* if

$$f(x_1, \dots, x_n; y_1, \dots, y_n) = f(x_{\pi(1)}, \dots, x_{\pi(n)}; y_{\tau(1)}, \dots, y_{\tau(n)})$$

for every pair of permutations  $\pi$  and  $\tau$  on  $\{1, \dots, n\}$ .

**Theorem 1.8.** *Every symmetric function  $f$  in  $R[x_1, \dots, x_n; y_1, \dots, y_n]$  can be written uniquely as a polynomial with coefficients in  $R$  in the elementary symmetric functions  $s_1, \dots, s_n$  and  $\sigma_1, \dots, \sigma_n$ .*

**Proof.** Use Theorem 1.4 twice. The details are left to the reader as an easy exercise. □

**Example 1.9.** The coefficient of each  $t^k$  in

$$h(t) = \prod_{i,j=1}^n (1 + x_i y_j t)$$

is a symmetric function on the  $x_i$ 's and the  $y_j$ 's. Therefore, it must be a polynomial in the elementary symmetric functions  $s_1, \dots, s_n$  and  $\sigma_1, \dots, \sigma_n$ . For example, a little bit of computation shows that

$$\begin{aligned} \prod_{i,j=1}^2 (1 + x_i y_j t) &= 1 + (s_1 \sigma_1) t + (s_1^2 \sigma_2 + s_2 \sigma_1^2 - 2s_2 \sigma_2) t^2 \\ &\quad + (s_1 s_2 \sigma_1 \sigma_2) t^3 + (s_2^2 \sigma_2^2) t^4. \end{aligned}$$

The reader should check this.

In general, the coefficient of  $t^n$  in  $h(t) = \prod_{i,j=1}^n (1 + x_i y_j t)$  is of the form

$$P_n(s_1, \dots, s_n; \sigma_1, \dots, \sigma_n)$$

for some universal polynomial  $P_n$  in  $2n$  variables with integer coefficients. For example, we have

$$\begin{aligned} P_1(x; y) &= xy, \\ P_2(x_1, x_2; y_1, y_2) &= x_1^2 y_2 + x_2 y_1^2 - 2x_2 y_2. \end{aligned}$$

These polynomials  $P_n$  will appear in the definition of a  $\lambda$ -ring (Definition 1.10).

## 1.2 $\lambda$ -Rings

The definition of a  $\lambda$ -ring involves certain axioms about the operations  $\lambda^0$ ,  $\lambda^1$ ,  $\lambda^n(x+y)$ ,  $\lambda^n(xy)$ , and  $\lambda^m(\lambda^n(x))$ . Before giving the exact definition, let us provide some motivation for the axioms.

### 1.2.1 The $\lambda$ -ring $\mathbf{Z}$

The simplest  $\lambda$ -ring is the ring of integers  $\mathbf{Z}$ , in which

$$\lambda^i(n) = \binom{n}{i} = \frac{n!}{i!(n-i)!}$$

for positive integers  $n$ . The corresponding generating function is

$$\lambda_t(n) = \sum_{i=0}^{\infty} \lambda^i(n)t^i = (1+t)^n,$$

which applies to all integers  $n$ . In other words,  $\lambda^i(n)$  is the coefficient of  $t^i$  in  $\lambda_t(n)$ . Since

$$(1+t)^n = 1 + nt + \dots,$$

we have  $\lambda^0(n) = 1$ ,  $\lambda^1(n) = n$ , and  $\lambda_t(1) = 1+t$ . Given two integers  $m$  and  $n$ , we have

$$\begin{aligned} \lambda_t(m+n) &= (1+t)^{m+n} \\ &= (1+t)^m(1+t)^n \\ &= \lambda_t(m)\lambda_t(n). \end{aligned}$$

So

$$\lambda^k(m+n) = \sum_{i+j=k} \lambda^i(m)\lambda^j(n),$$

which expresses  $\lambda^k$  of a sum in terms of the individual  $\lambda^i$ . Furthermore, a little bit of computation shows that

$$\begin{aligned} \binom{mn}{2} &= m^2 \binom{n}{2} + n^2 \binom{m}{2} - 2 \binom{m}{2} \binom{n}{2}, \\ \binom{\binom{n}{2}}{2} &= n \binom{n}{3} - \binom{n}{4}. \end{aligned}$$

It follows that

$$\begin{aligned} \lambda^2(mn) &= (\lambda^1(m))^2 \lambda^2(n) + (\lambda^1(n))^2 \lambda^2(m) - 2\lambda^2(m)\lambda^2(n), \\ \lambda^2(\lambda^2(n)) &= \lambda^1(n)\lambda^3(n) - \lambda^4(n). \end{aligned}$$

In general,  $\lambda^k(mn)$  is a polynomial with integer coefficients in  $\lambda^1(m), \dots, \lambda^k(m), \lambda^1(n), \dots, \lambda^k(n)$ . Likewise,  $\lambda^i(\lambda^j(n))$  is a polynomial with integer coefficients in  $\lambda^1(n), \dots, \lambda^{ij}(n)$ .

With the above example in mind, we now give the definition of a  $\lambda$ -ring.

### 1.2.2 Basic properties of $\lambda$ -rings

**Definition 1.10.** A  $\lambda$ -ring is a ring  $R$  together with functions

$$\lambda^n: R \rightarrow R \quad (n \geq 0),$$

called  $\lambda$ -operations, such that for all  $x, y \in R$ , the following axioms are satisfied:

- (1)  $\lambda^0(x) = 1$ ,
- (2)  $\lambda^1(x) = x$ ,
- (3)  $\lambda^n(1) = 0$  for  $n \geq 2$ ,
- (4)  $\lambda^n(x + y) = \sum_{i+j=n} \lambda^i(x)\lambda^j(y)$ ,
- (5)  $\lambda^n(xy) = P_n(\lambda^1(x), \dots, \lambda^n(x); \lambda^1(y), \dots, \lambda^n(y))$ ,
- (6)  $\lambda^n(\lambda^m(x)) = P_{n,m}(\lambda^1(x), \dots, \lambda^{nm}(x))$ .

Here  $P_n$  and  $P_{n,m}$  are the universal polynomials with integer coefficients from Example 1.9 and Example 1.7, respectively. If only axioms (1), (2), and (4) are satisfied, then we call  $R$  a *pre- $\lambda$ -ring*.

In a (pre-) $\lambda$ -ring  $R$ , we write

$$\lambda_t(x) = \sum_{n=0}^{\infty} \lambda^n(x)t^n, \quad (1.7)$$

considered as a formal power series in  $t$  with coefficients in  $R$ . Using this notation, we can rewrite axiom (4) above as

$$\lambda_t(x + y) = \lambda_t(x)\lambda_t(y). \quad (1.8)$$

**Definition 1.11.** If  $\lambda_t(x)$  is a polynomial of degree  $n$ , then we say that  $x$  has *dimension  $n$*  and write  $\dim(x) = n$ . If every element in  $R$  is the difference of finite dimensional elements, then we say that  $R$  is *finite dimensional*.

**Remark 1.12.** What we call a  $\lambda$ -ring (pre- $\lambda$ -ring) here used to be called a *special  $\lambda$ -ring* ( $\lambda$ -ring) in [Atiyah and Tall (1969); Berthelot *et al.* (1971); Fulton and Lang (1985); Grothendieck (1971)]. Our terminology follows that in [Knutson (1973)]. Also, the dimension of an element in a  $\lambda$ -ring was called the *degree* of that element in [Knutson (1973)].

In Proposition 2.8 and Corollary 2.10 below, we will provide some criteria that make a pre- $\lambda$ -ring into a  $\lambda$ -ring.

Here are some of the most basic properties of a  $\lambda$ -ring.

**Proposition 1.13.** *Let  $R$  be a  $\lambda$ -ring, and let  $x$  and  $y$  be elements in  $R$ . Then the following statements hold.*

- (1)  $\lambda_t(1) = 1 + t$ .
- (2)  $\lambda_t(0) = 1$ .
- (3)  $\lambda_t(x + y) = \lambda_t(x)\lambda_t(y)$ .

$$(4) \lambda_t(-x) = \lambda_t(x)^{-1}.$$

$$(5) \dim(x + y) \leq \dim(x) + \dim(y).$$

(6) If  $x$  and  $y$  are both 1-dimensional, then so is  $xy$ . So a finite product of 1-dimensional elements is again 1-dimensional.

**Proof.** All the statements are immediate from the  $\lambda$ -ring axioms. For example, assuming (2) and (3) we have

$$\begin{aligned} 1 &= \lambda_t(0) \\ &= \lambda_t(x - x) \\ &= \lambda_t(x)\lambda_t(-x), \end{aligned}$$

which proves (4).

For statement (6), suppose that  $n \geq 2$ . In the product

$$h(t) = \prod_{i,j=1}^n (1 + x_i y_j t),$$

set  $x_2, \dots, x_n, y_2, \dots, y_n$  to 0. Then direct inspection shows that the coefficient of  $t^n$  is 0. This implies that

$$P_n(s_1, 0, 0, \dots; \sigma_1, 0, 0, \dots) = 0,$$

which in turn implies that

$$\lambda^n(xy) = P_n(\lambda^1(x), 0, 0, \dots; \lambda^1(y), 0, 0, \dots) = 0.$$

Therefore, the product  $xy$  is 1-dimensional. The proofs of the other statements are left as exercises.  $\square$

**Proposition 1.14.** *The following statements hold in a  $\lambda$ -ring  $R$  for  $k \geq 1$  and  $a, a_1, \dots, a_n \in R$ :*

$$\lambda^k(a_1 + \dots + a_n) = \sum_{i=1}^n \lambda^k(a_i) + (\text{polynomial in } \lambda^j(a_l), j < k, 1 \leq l \leq n),$$

$$\lambda^k(-a) = -\lambda^k(a) + (\text{polynomial in } \lambda^j(a), j < k).$$

Here by “polynomial” we mean a polynomial with integer coefficients.

**Proof.** The first assertion follows from the equality

$$\lambda^k(a_1 + \dots + a_n) = \sum_{k_1 + \dots + k_n = k} \lambda^{k_1}(a_1) \dots \lambda^{k_n}(a_n)$$

and the axiom  $\lambda^0(x) = 1$ . For the second assertion, we have

$$\begin{aligned} 0 &= \lambda^k(a + (-a)) \\ &= \lambda^k(a) + \lambda^k(-a) + (\text{polynomial in } \lambda^i(a), \lambda^i(-a), i < k). \end{aligned}$$

Thus, we have

$$\lambda^k(-a) = -\lambda^k(a) + (\text{polynomial in } \lambda^i(a), \lambda^i(-a), i < k).$$

Now apply the same procedure to the terms  $\lambda^i(-a)$  ( $i < k$ ), and so forth. The second assertion of the Lemma follows by a finite downward induction.  $\square$

### 1.2.3 Examples of $\lambda$ -rings

**Example 1.15.** The ring  $\mathbf{Z}$  of integers is a finite-dimensional  $\lambda$ -ring with

$$\lambda_t(n) = (1 + t)^n$$

for  $n \in \mathbf{Z}$ , i.e.,

$$\lambda^i(n) = \text{coefficient of } t^i \text{ in } (1 + t)^n.$$

Indeed, we have already seen that axioms (1) to (4) are satisfied. Axioms (5) and (6) are certain universal identities about the binomial coefficients. It is possible to prove them directly. However, it is easier to verify them using the universal  $\lambda$ -ring (Corollary 2.11).

Notice that an integer  $n \geq 0$  has dimension  $n$ , while negative integers do not have finite dimensions.

**Example 1.16.** The topological  $K$ -theory  $K(X)$  of any nice-enough space  $X$  (e.g., para-compact Hausdorff space) is a  $\lambda$ -ring [Atiyah (1989); Atiyah and Tall (1969)], in which  $\lambda^i$  is induced by the  $i$ th exterior power on vector bundles over  $X$ . Moreover, the  $K$ -theory of a point (or any contractible space) is  $K(pt.) \cong \mathbf{Z}$  as a  $\lambda$ -ring. Moreover, if  $X$  is a finite CW complex, then  $K(X)$  is a finite-dimensional  $\lambda$ -ring.

**Example 1.17.** For a group  $G$ , the complex representation ring  $R(G)$  is a  $\lambda$ -ring [Atiyah and Tall (1969)], in which  $\lambda^i$  is induced by the  $i$ th exterior power on representations of  $G$ . The  $\lambda$ -ring  $R(G)$  is finite-dimensional if  $G$  is a finite group. Moreover, if  $G = \{e\}$  is the trivial group, then  $R(\{e\}) \cong \mathbf{Z}$  as a  $\lambda$ -ring. As we will see in §5.5, the trivial group is the *only* finite group whose representation ring is isomorphic to  $\mathbf{Z}$ . This is a consequence of Knutson's Theorem 5.36.

A lot more examples of  $\lambda$ -rings will be given in the following chapters when we have the universal  $\lambda$ -ring and Adams operations at our disposal. Here is a preview of some of them.

**Example 1.18.** Let  $R$  be a ring. Then its *universal  $\lambda$ -ring*  $\Lambda(R)$  is always a  $\lambda$ -ring (Theorem 2.6).

**Example 1.19.** Let  $R$  be a ring. Then the ring  $\mathbf{W}(R)$  of *big Witt vectors on  $R$*  is a  $\lambda$ -ring, which is isomorphic to  $\Lambda(R)$  (Theorem 4.16) via the Artin-Hasse Exponential isomorphism.

**Example 1.20.** The ring  $\hat{\mathbf{Z}}_p$  of  $p$ -adic integers is a  $\lambda$ -ring (Corollary 3.63), as is the ring  $\mathbf{Z}_{(p)}$  of  $p$ -local integers (Corollary 3.59).

**Example 1.21.** Let  $G$  be a group, and let  $\mathbf{k}$  be a field of characteristic 0. Let  $C_G$  be the set of conjugacy classes of  $G$ , and let  $\mathbf{k}(C_G)$  be the ring of central functions on  $G$  with values in  $\mathbf{k}$ . Then  $\mathbf{k}(C_G)$  is a  $\lambda$ -ring (Chapter 3 Exercise (7d)).

**Example 1.22.** Every *binomial ring* is a  $\lambda$ -ring (Theorem 5.3). In particular, every ring  $\text{Int}(\mathbf{Z}^X)$  of *integer-valued polynomials* is a  $\lambda$ -ring (Theorem 5.21).

**Example 1.23.** For a binomial ring  $R$ , its *necklace ring*  $Nr(R)$  is a  $\lambda$ -ring (Corollary 5.45).

**Example 1.24.** Many quotients of the power series ring  $\mathbf{Z}[[x_1, \dots, x_n]]$  are  $\lambda$ -rings (Theorem 6.13).

### 1.2.4 Homomorphisms and ideals

**Definition 1.25.** Let  $R$  and  $S$  be (pre-) $\lambda$ -rings.

- (1) A (pre-) $\lambda$ -homomorphism  $f: R \rightarrow S$  is a ring homomorphism such that  $f\lambda^i = \lambda^i f$  for  $i \geq 0$ .
- (2) A (pre-) $\lambda$ -ideal in  $R$  is an ideal  $I$  in  $R$  such that  $\lambda^i(x) \in I$  for  $i \geq 1$  and  $x \in I$ .
- (3) A (pre-) $\lambda$ -subring of  $R$  is a subring  $R'$  of  $R$  such that  $\lambda^i(x) \in R'$  for all  $i \geq 0$  and  $x \in R'$ .

**Example 1.26.**

- (1) If  $f: X \rightarrow Y$  is a map of topological spaces, then the induced map  $K(f): K(Y) \rightarrow K(X)$  on  $K$ -theory is a  $\lambda$ -homomorphism.
- (2) If  $\varphi: G \rightarrow H$  is a group homomorphism, then the induced map  $R(\varphi): R(H) \rightarrow R(G)$  on the representation rings is a  $\lambda$ -homomorphism.

The usual properties and constructions of rings extend in an obvious way to  $\lambda$ -rings.

**Proposition 1.27.** Let  $R$  and  $S$  be  $\lambda$ -rings, and let  $f: R \rightarrow S$  be a  $\lambda$ -homomorphism.

- (1) The kernel of  $f$  is a  $\lambda$ -ideal in  $R$ .
- (2) The image of  $f$  is a  $\lambda$ -subring in  $S$ .
- (3) The quotient  $R/I$  of  $R$  by a  $\lambda$ -ideal  $I$  is naturally a  $\lambda$ -ring, and the projection map  $R \rightarrow R/I$  is a  $\lambda$ -homomorphism.
- (4) The direct product  $R \times S$  is a  $\lambda$ -ring, in which

$$\lambda_t(r, 0) = (1, 1) + \sum_{n \geq 1} (\lambda^n(r), 0)t^n,$$

$$\lambda_t(0, s) = (1, 1) + \sum_{n \geq 1} (0, \lambda^n(s))t^n,$$

$$\lambda_t(r, s) = \lambda_t(r, 0)\lambda_t(0, s).$$

(5) The tensor product  $R \otimes S$  is a  $\lambda$ -ring, in which

$$\begin{aligned}\lambda^n(r \otimes 1) &= \lambda^n(r) \otimes 1, \\ \lambda^n(1 \otimes s) &= 1 \otimes \lambda^n(s), \\ \lambda^n(r \otimes s) &= \lambda^n((r \otimes 1)(1 \otimes s)).\end{aligned}$$

(6) If  $\{R_\alpha\}$  is an inverse system of  $\lambda$ -rings, then the inverse limit ring  $\varprojlim_\alpha R_\alpha$  is naturally a  $\lambda$ -ring.

**Proof.** Straightforward exercise. □

An ideal in a ring is often described by a set of generators. To check that an ideal  $I$  in a  $\lambda$ -ring  $R$  is a  $\lambda$ -ideal, one would have to check that  $\lambda^n(x) \in I$  for  $n \geq 1$  and all  $x \in I$ . The following result reduces this process to just checking the generators.

**Proposition 1.28.** *Let  $R$  be a  $\lambda$ -ring, and let  $I$  be an ideal in  $R$  generated by  $\{z_j\}_{j \in J}$ . Then  $I$  is a  $\lambda$ -ideal if and only if  $\lambda^n(z_j) \in I$  for  $n \geq 1$  and  $j \in J$ .*

**Proof.** The “only if” part is obvious. For the other direction, first consider an element in  $I$  of the form  $rz$  for some  $r \in R$  and  $z \in \{z_j\}_{j \in J}$ . In the polynomial

$$h(t) = \prod_{i,j=1}^n (1 + x_i y_j t),$$

if one sets all the  $y_j$  to 0, then the coefficient of  $t^n$  is 0. This implies that

$$P_n(s_1, \dots, s_n; 0, 0, \dots, 0) = 0,$$

which in turn implies that every non-zero term in  $P_n(s_1, \dots, s_n; \sigma_1, \dots, \sigma_n)$  contains a factor of  $\sigma_k$  for some  $k$ . It follows that the element

$$\lambda^n(rz) = P_n(\lambda^1(r), \dots, \lambda^n(r); \lambda^1(z), \dots, \lambda^n(z))$$

is a finite sum of terms, each one containing a factor of  $\lambda^k(z) \in I$  for some  $k$ . So  $\lambda^n(rz)$  lies in  $I$  as well.

A general element in  $I$  is a linear combination  $w = \sum_{k=1}^m r_k z_{j_k}$  with coefficients in  $R$ . To show that  $\lambda^n(w) \in I$  for  $n \geq 1$ , note that by Proposition 1.13 (3) one has  $\lambda_t(w) = \prod_{k=1}^m \lambda_t(r_k z_{j_k})$ . Therefore, each  $\lambda^n(w)$  is a finite sum of products of  $\lambda^p(r_k z_{j_k}) \in I$  for various  $p$  and  $k$ . This shows that  $\lambda^n(w)$  lies in  $I$ . □

It was mentioned earlier that  $\mathbf{Z}$  is the simplest  $\lambda$ -ring. The following result is the reason for that assertion.

**Proposition 1.29.** *The following statements hold.*

- (1) The ring  $\mathbf{Z}$  has a unique  $\lambda$ -ring structure with  $\lambda_t(m) = (1 + t)^m$  for  $m \in \mathbf{Z}$ .
- (2) Every  $\lambda$ -ring has characteristic 0.
- (3) Every  $\lambda$ -ring contains a  $\lambda$ -subring that is isomorphic to  $\mathbf{Z}$ .

**Proof.** In any  $\lambda$ -ring, one has  $\lambda_t(1) = 1 + t$ . Therefore, for a positive integer  $m$  one has that

$$\lambda_t(m) = \lambda_t(\underbrace{1 + \cdots + 1}_{m \text{ times}}) = \lambda_t(1)^m = (1 + t)^m.$$

Moreover, by Proposition 1.13 (4) one has

$$\lambda_t(-m) = \lambda_t(m)^{-1} = (1 + t)^{-m},$$

which shows that the stated  $\lambda$ -ring structure on  $\mathbf{Z}$  is the only one.

In a  $\lambda$ -ring  $R$ , for a positive integer  $m$ , a similar calculation as above shows that

$$\lambda_t(m \cdot 1) = \lambda_t(\underbrace{1 + \cdots + 1}_{m \text{ times}}) = (1 + t)^m = 1 + \cdots + t^m.$$

This is a polynomial of degree  $m$  over any ring, which shows that  $m \neq 0$  in  $R$ . Therefore,  $R$  has characteristic 0 and has a  $\lambda$ -subring isomorphic to  $\mathbf{Z}$ .  $\square$

### 1.2.5 Augmented $\lambda$ -rings

Many  $\lambda$ -rings in practice come with a  $\lambda$ -homomorphism to  $\mathbf{Z}$ . We give these  $\lambda$ -rings a special name.

**Definition 1.30.** An *augmented  $\lambda$ -ring* is a  $\lambda$ -ring  $R$  that comes equipped with a  $\lambda$ -homomorphism  $\varepsilon: R \rightarrow \mathbf{Z}$ , called the *augmentation*.

**Example 1.31.** If  $x_0$  is a base point of a topological space  $X$ , then the  $K$ -theory  $K(X)$  of  $X$  is an augmented  $\lambda$ -ring. The augmentation  $\varepsilon: K(X) \rightarrow \mathbf{Z}$  is induced by the map that sends an actual vector bundle over  $X$  to the dimension of the fiber over  $x_0$ .

**Example 1.32.** The representation ring  $R(G)$  of a group  $G$  is an augmented  $\lambda$ -ring. The augmentation  $\varepsilon: R(G) \rightarrow \mathbf{Z}$  is induced by the map that sends an actual representation to its dimension.

Augmented  $\lambda$ -rings admit a natural decomposition with  $\mathbf{Z}$  as a factor.

**Proposition 1.33.** *The following statements hold.*

(1) *If  $R$  is an augmented  $\lambda$ -ring with augmentation  $\varepsilon$ , then*

$$0 \leq \varepsilon(x) \leq \dim(x)$$

*for any finite dimensional element  $x \in R$ .*

(2) *A  $\lambda$ -ring  $R$  is augmented if and only if there exists a  $\lambda$ -ideal  $I$  such that  $R = \mathbf{Z} \oplus I$  as an abelian group.*

(3) *If  $R$  and  $S$  are augmented  $\lambda$ -rings, then  $R \otimes S$  is also an augmented  $\lambda$ -ring.*

**Proof.** If  $x \in R$  is of finite dimension  $d$ , then for any integer  $n > d$  one has that

$$\lambda^n(\varepsilon(x)) = \varepsilon(\lambda^n(x)) = \varepsilon(0) = 0.$$

This shows that  $\varepsilon(x) \leq d$  and is non-negative.

For the second statement, suppose that  $R$  is augmented with augmentation  $\varepsilon$ . Let  $I$  denote the kernel of  $\varepsilon$ . Given any element  $x \in R$ , one can always write it uniquely as

$$x = \varepsilon(x) + (x - \varepsilon(x)),$$

in which  $\varepsilon(x) \in \mathbf{Z}$  and  $(x - \varepsilon(x)) \in I$ . This shows that  $R$  decomposes as  $\mathbf{Z} \oplus I$ . Conversely, if there exists a  $\lambda$ -ideal  $I$  such that  $R = \mathbf{Z} \oplus I$  as an abelian group, then  $R$  is augmented by the projection map onto the first factor.

The tensor product  $R \otimes S$  is a  $\lambda$ -ring by Proposition 1.27. If the augmentations of  $R$  and  $S$  are  $\varepsilon_R$  and  $\varepsilon_S$ , respectively, then  $R \otimes S$  has augmentation  $\varepsilon_R \otimes \varepsilon_S$ .  $\square$

Given a  $\lambda$ -ring  $R$ , it is convenient to know how to put a  $\lambda$ -ring structure on the polynomial ring  $R[x]$  or the power series ring  $R[[x]]$ . This is illustrated by the following result.

**Proposition 1.34.** *Let  $R$  be a  $\lambda$ -ring. Then there exists a unique  $\lambda$ -ring structure on the polynomial ring  $R[x]$  such that  $\lambda_t(x) = 1 + xt$ , i.e.,  $\dim(x) = 1$ . If  $R$  is augmented, then so is  $R[x]$  with  $\varepsilon(x) = 0$  or  $1$ . The same holds for the power series ring  $R[[x]]$ .*

**Proof.** We take  $\lambda_t(x) = 1 + xt$  as a definition and extend it to all of  $R[x]$  or  $R[[x]]$  as follows. The  $\lambda$ -operations are extended to the powers  $x^i$  using the  $\lambda$ -ring axiom for  $\lambda^n(xy)$  repeatedly. For an element  $r \in R$ , we use this axiom again to extend the  $\lambda$ -operations to monomials of the form  $rx^i$ . For a polynomial (or formal power series)  $f = \sum_i r_i x^i$  with coefficients in  $R$ , we define

$$\lambda_t(f) = \prod_i \lambda_t(r_i x^i)$$

using the axiom for  $\lambda^n(x + y)$ . The same reasoning shows that the  $\lambda$ -ring structure is uniquely determined by the condition  $\lambda_t(x) = 1 + xt$ . The assertion about the augmentation is clear.  $\square$

We will use this result below in the construction of the free  $\lambda$ -ring on one generator. Applying Proposition 1.34 repeatedly, we obtain the following result.

**Corollary 1.35.** *Let  $R$  be a  $\lambda$ -ring. Then there exists a unique  $\lambda$ -ring structure on the polynomial ring  $R[x_1, \dots, x_n]$  on  $n$  variables such that  $\lambda_t(x_i) = 1 + x_i t$  for  $1 \leq i \leq n$ , i.e.,  $\dim(x_i) = 1$  for each  $i$ . If  $R$  is augmented, then so is  $R[x_1, \dots, x_n]$  with  $\varepsilon(x_i) = 0$  or  $1$  for each  $i$ . The same holds for the power series ring  $R[[x_1, \dots, x_n]]$  on  $n$  variables.*

**Proof.** Apply Proposition 1.34  $n$  times.  $\square$

### 1.3 Free $\lambda$ -Rings

In this section we construct the free  $\lambda$ -ring  $U$  on one generator. This ring  $U$  also occurs in (at least) two other places. First,  $U$  is also the ring of operations on  $\lambda$ -rings, which we will discuss in §1.4. Second, in representation theory, the ring  $U$  is often called the *ring of symmetric functions*. In fact,  $U$  is isomorphic to the graded ring

$$R(S) = \bigoplus_{n=0}^{\infty} R(S_n),$$

in which  $R(S_n)$  is the representation ring of the symmetric group  $S_n$  on  $n$  letters [Knutson (1973)].

Before we construct  $U$ , let us provide some motivation for its construction. Since  $U$  is to be the free  $\lambda$ -ring on one generator, say,  $x$ , it should have the following universal property. Given any  $\lambda$ -ring  $R$  and an element  $r \in R$ , there exists a unique  $\lambda$ -homomorphism  $u_r: U \rightarrow R$  such that  $u_r(x) = r$ . Because  $U$  is a  $\lambda$ -ring itself, it should also contain  $\lambda^n(x)$  for  $n \geq 1$ . Therefore, it contains all the polynomials with integer coefficients in  $x, \lambda^2(x), \lambda^3(x)$ , etc., and hence also the ring

$$U' = \mathbf{Z}[x, \lambda^2(x), \lambda^3(x), \dots].$$

This latter ring  $U'$  is already a  $\lambda$ -ring because of the  $\lambda$ -ring axiom for  $\lambda^m(\lambda^n(x))$ , which expresses it as a polynomial with integer coefficients in  $\lambda^i(x)$  ( $1 \leq i \leq mn$ ). So  $U'$  is a  $\lambda$ -subring of  $U$  containing  $x$ , which implies that  $U$  should be equal to  $U'$ .

It turns out that the elements  $\lambda^i(x)$  ( $i \geq 1$ ) in  $U$  must also be algebraically independent. In other words,  $U$  is a polynomial ring over  $\mathbf{Z}$  in countably infinitely many variables  $y_1, y_2, \dots$  such that  $\lambda^n(y_1) = y_n$ .

We now give the exact construction of  $U$ .

#### 1.3.1 The free $\lambda$ -ring on one generator

Let  $x_1, x_2, \dots$  be an infinite sequence of algebraically independent variables. Consider the polynomial ring

$$\Omega_r = \mathbf{Z}[x_1, \dots, x_r]$$

in  $r \geq 0$  variables. Since  $\mathbf{Z}$  is a  $\lambda$ -ring (Proposition 1.29), by Corollary 1.35 there exists a unique  $\lambda$ -ring structure on  $\Omega_r$  in which  $\lambda_t(x_i) = 1 + x_i t$ , i.e., each  $x_i$  has dimension 1.

These  $\lambda$ -rings fit into an inverse system

$$\mathbf{Z} = \Omega_0 \xleftarrow{p_1} \Omega_1 \xleftarrow{p_2} \Omega_2 \xleftarrow{p_3} \Omega_3 \xleftarrow{p_4} \dots, \tag{1.9}$$

in which the  $\lambda$ -homomorphism

$$p_{r+1}: \Omega_{r+1} \rightarrow \Omega_r \tag{1.10}$$

is defined by

$$p_{r+1}(x_i) = \begin{cases} x_i & \text{if } 1 \leq i \leq r, \\ 0 & \text{if } i = r + 1. \end{cases}$$

Define

$$\Omega = \varprojlim \Omega_r, \quad (1.11)$$

the inverse limit of the inverse system (1.9). Let  $\phi_r: \Omega \rightarrow \Omega_r$  be the structure map that comes with the inverse limit. By Proposition 1.27,  $\Omega$  is a  $\lambda$ -ring, and  $\phi_r$  is a  $\lambda$ -homomorphism. From the definition of inverse limit, an element in  $\Omega$  is a power series  $f$  with integer coefficients in the variables  $x_i$  ( $i \geq 1$ ) such that for each  $r \geq 1$ ,

$$\phi_r(f) = f(x_1, \dots, x_r, 0, 0, \dots)$$

is a polynomial in  $x_1, \dots, x_r$ .

Let  $s_n(x_1, \dots, x_r)$  be the  $n$ th elementary symmetric function on  $x_1, \dots, x_r$  (Example 1.1). Since

$$\begin{aligned} s_n(x_1, \dots, x_r, 0) &= p_{r+1}(s_n(x_1, \dots, x_{r+1})) \\ &= s_n(x_1, \dots, x_r), \end{aligned}$$

the sequence  $\{s_n(x_1, \dots, x_r)\}_{r \geq 0}$  determines an element

$$s_n = \varprojlim_r s_n(x_1, \dots, x_r)$$

in  $\Omega$ . Thinking of  $s_n$  as a power series, we have

$$\begin{aligned} s_n &= \sum_{i_1 < \dots < i_n} x_{i_1} \cdots x_{i_n}, \\ \phi_r(s_n) &= s_n(x_1, \dots, x_r) = \sum_{1 \leq i_1 < \dots < i_n \leq r} x_{i_1} \cdots x_{i_n}. \end{aligned} \quad (1.12)$$

For example,  $s_1$  is the infinite sum  $s_1 = x_1 + x_2 + x_3 + \dots$ , and  $\phi_r(s_1) = x_1 + \dots + x_r$  for each  $r \geq 1$ .

In view of the above discussion, we think of  $s_n$  as the  $n$ th elementary symmetric function on a countable set of variables  $x_i$  ( $i \geq 1$ ). Therefore, we can write down the generating function for these elementary symmetric functions formally as

$$1 + \sum_{n=1}^{\infty} s_n t^n = \prod_{i=1}^{\infty} (1 + x_i t). \quad (1.13)$$

This is the analog of (1.2) involving countably infinitely many variables. There is an obvious analog of The Fundamental Theorem of Symmetric Functions (Theorem 1.4) that involves an infinite sequence of variables  $x_i$  ( $i \geq 1$ ), with  $s_n$  (1.12) playing the role of the  $n$ th elementary symmetric function.

**Proposition 1.36.** *In the  $\lambda$ -ring  $\Omega$ , the elements  $s_n$  ( $n \geq 1$ ) are algebraically independent. Moreover, one has  $\lambda^n(s_1) = s_n$  for  $n \geq 1$ .*

**Proof.** Suppose that  $f(s_1, \dots, s_n) = 0$  is a polynomial relation involving  $s_1, \dots, s_n$ . Then

$$\begin{aligned} 0 &= \phi_n f(s_1, \dots, s_n) \\ &= f(\phi_n(s_1), \dots, \phi_n(s_n)) \\ &= f(s_1(x_1, \dots, x_n), \dots, s_n(x_1, \dots, x_n)). \end{aligned}$$

The algebraic independence of  $s_i(x_1, \dots, x_n)$  ( $1 \leq i \leq n$ ) (Theorem 1.4) then shows that  $f$  is the 0 polynomial. This proves that the elements  $s_n$  ( $n \geq 1$ ) are algebraically independent.

For the second assertion, note that for  $r \geq n$ , one has

$$\begin{aligned} \phi_r \lambda^n(s_1) &= \lambda^n(\phi_r(s_1)) \\ &= \lambda^n(x_1 + \dots + x_r) \\ &= \sum_{1 \leq i_1 < \dots < i_n \leq r} x_{i_1} \cdots x_{i_n} \\ &= \phi_r(s_n). \end{aligned}$$

The third equality is a consequence of the  $\lambda$ -ring axiom for  $\lambda^n(x + y)$  and the fact that  $\dim(x_i) = 1$  for each  $i$ . Since this holds for all  $r \geq n$ , it follows that  $\lambda^n(s_1) = s_n$ , as desired.  $\square$

**Definition 1.37.** Let  $U$  be the smallest  $\lambda$ -subring of  $\Omega$  that contains  $s_1$ . The  $\lambda$ -ring  $U$  is called the *free  $\lambda$ -ring on one generator*.

**Proposition 1.38.** *The free  $\lambda$ -ring on one generator is the polynomial ring*

$$U = \mathbf{Z}[s_1, s_2, s_3, \dots]$$

*on the algebraically independent elements  $s_i$  ( $i \geq 1$ ).*

**Proof.** Since  $s_1 \in U$ , so is  $\lambda^n(s_1) = s_n$  (Proposition 1.36). It follows that  $U$  contains the stated polynomial ring. The latter is closed under the  $\lambda$ -operations by the  $\lambda$ -ring axiom on  $\lambda^m(\lambda^n(x))$ , so it is a  $\lambda$ -ring. Therefore, it must be equal to the ring  $U$ .  $\square$

We now show that  $U$  has the right universal property.

**Theorem 1.39.** *Let  $R$  be a  $\lambda$ -ring, and let  $r$  be an element in  $R$ . Then there exists a unique  $\lambda$ -homomorphism  $u_r: U \rightarrow R$  such that  $\lambda^n(r) = u_r(s_n)$  for  $n \geq 1$ .*

**Proof.** Define a ring homomorphism  $u_r: U \rightarrow R$  by first setting  $u_r(s_1) = r$ . This extends uniquely to a  $\lambda$ -homomorphism on  $U$ , since, to be such,  $u_r$  must satisfy

$$\lambda^n(r) = \lambda^n(u_r(s_1)) = u_r(\lambda^n(s_1)) = u_r(s_n).$$

So we must choose  $u_r(s_n)$  to be  $\lambda^n(r)$ .  $\square$

One can construct the free  $\lambda$ -ring on any set of generators following the procedure above. We leave it to the reader to work out the details in the exercises.

### 1.4 The Verification Principle

In this section we prove The Verification Principle, which states that a natural operation on  $\lambda$ -rings is uniquely determined by its action on sums of 1-dimensional elements. We begin by defining natural operations on  $\lambda$ -rings.

**Definition 1.40.** By a *natural operation on  $\lambda$ -rings*, we mean a rule that assigns to each  $\lambda$ -ring  $R$  a function (not necessarily a  $\lambda$ -homomorphism)  $\mu_R: R \rightarrow R$  such that, if  $f: R \rightarrow S$  is a  $\lambda$ -homomorphism, then the square

$$\begin{array}{ccc}
 R & \xrightarrow{f} & S \\
 \mu_R \downarrow & & \downarrow \mu_S \\
 R & \xrightarrow{f} & S
 \end{array}$$

commutes.

Natural operations on  $\lambda$ -rings can be added and multiplied in the obvious way:

$$\begin{aligned}
 (\mu + \nu)_R(r) &= \mu_R(r) + \nu_R(r), \\
 (\mu\nu)_R(r) &= \mu_R(r)\nu_R(r).
 \end{aligned}$$

In particular, the set of all natural operations on  $\lambda$ -rings is a ring, which is denoted by  $Op^\lambda$ .

**Example 1.41.** From the definition of a  $\lambda$ -homomorphism, each  $\lambda$ -operation  $\lambda^i$  ( $i \geq 0$ ) is a natural operation on  $\lambda$ -rings. It follows that any monomial of the  $\lambda$ -operations,  $\lambda^{i_1} \cdots \lambda^{i_n}$ , is a natural operation on  $\lambda$ -rings as well. Going one step further, any polynomial with integer coefficients in the  $\lambda$ -operations is a natural operation on  $\lambda$ -rings. We denote this latter ring by  $\mathbf{Z}[\lambda^1, \lambda^2, \lambda^3, \dots]$ . Therefore, there is a ring homomorphism

$$\alpha: \mathbf{Z}[\lambda^1, \lambda^2, \lambda^3, \dots] \rightarrow Op^\lambda \tag{1.14}$$

given by  $\alpha(f(\lambda^1, \dots, \lambda^n))_R(r) = f(\lambda^1(r), \dots, \lambda^n(r))$  for an element  $r$  in a  $\lambda$ -ring  $R$ .

We now show that every natural operation on  $\lambda$ -rings can be expressed uniquely as a polynomial with integer coefficients in the  $\lambda$ -operations.

**Theorem 1.42.** *The map  $\alpha$  (1.14) is a ring isomorphism.*

**Proof.** Since  $\alpha$  is clearly a ring homomorphism, it remains to show that  $\alpha$  is a bijection. To show that it is injective, suppose that  $\alpha(f(\lambda^1, \dots, \lambda^n)) = 0$ . When applied to the free  $\lambda$ -ring on one generator  $U$ , one has

$$\begin{aligned}
 0 &= \alpha(f(\lambda^1, \dots, \lambda^n))_U(s_1) \\
 &= f(\lambda^1(s_1), \dots, \lambda^n(s_1)) \\
 &= f(s_1, \dots, s_n).
 \end{aligned}$$

Since the  $s_i$  ( $i \geq 1$ ) are algebraically independent (Proposition 1.36), it follows that  $f = 0$ , showing that  $\alpha$  is injective.

To show that  $\alpha$  is surjective, let  $\mu$  be a natural operation on  $\lambda$ -rings. Applying it to  $U$  again, one has  $\mu_U(s_1) = g(s_1, \dots, s_n)$  for some polynomial  $g$  with integer coefficients. We claim that

$$\mu = \alpha(g(\lambda^1, \dots, \lambda^n)). \quad (1.15)$$

Indeed, if  $r$  is an element in a  $\lambda$ -ring  $R$ , then by Theorem 1.39 there exists a unique  $\lambda$ -homomorphism  $u_r: U \rightarrow R$  such that  $u_r(s_n) = \lambda^n(r)$  for all  $n \geq 1$ . Therefore, we have

$$\begin{aligned} \mu_R(r) &= \mu_R(u_r(s_1)) \\ &= u_r(\mu_U(s_1)) \\ &= u_r(g(s_1, \dots, s_n)) \\ &= g(u_r(s_1), \dots, u_r(s_n)) \\ &= g(\lambda^1(r), \dots, \lambda^n(r)). \end{aligned}$$

This establishes (1.15), showing that  $\alpha$  is surjective.  $\square$

We are now ready to prove the desired result.

**Theorem 1.43 (The Verification Principle).** *Every natural operation  $\mu$  on  $\lambda$ -rings is uniquely a polynomial with integer coefficients in the  $\lambda$ -operations. Moreover, one has*

$$\mu = f(\lambda^1, \dots, \lambda^n) \quad (1.16)$$

*if and only if this equality holds when applied to finite sums of 1-dimensional elements.*

**Proof.** The first assertion was proved in Theorem 1.42. As in the second paragraph of the proof of Theorem 1.42, the condition (1.16) holds if and only if  $\mu_U(s_1) = f(s_1, \dots, s_n)$ . It suffices to check this condition in  $\Omega$  (1.11), which is the inverse limit of  $\Omega_r$  ( $r \geq 0$ ). Therefore, it suffices to check this condition in each  $\Omega_r$ :

$$\begin{aligned} \mu_{\Omega_r}(x_1 + \dots + x_r) &= \mu_{\Omega_r}(\phi_r(s_1)) \\ &= f(\phi_r(s_1), \dots, \phi_r(s_n)) \\ &= f(s_1(x_1, \dots, x_r), \dots, s_n(x_1, \dots, x_r)). \end{aligned}$$

Since each  $x_i$  is 1-dimensional, the Theorem is proved.  $\square$

## 1.5 The Splitting Principle

The purpose of this section is to prove The Splitting Principle, which allows one to write an arbitrary finite dimensional element in a  $\lambda$ -ring as a sum of 1-dimensional elements in a possibly larger  $\lambda$ -ring.

The idea of The Splitting Principle is that, given an  $n$ -dimensional element  $x$  in a  $\lambda$ -ring  $R$ , one would like to write it as a sum

$$x = x_1 + \cdots + x_n$$

of  $n$  one-dimensional elements  $x_i$ . It proceeds by first adjoining an element  $x_1$  of dimension one to  $R$  such that  $\dim(x - x_1) = n - 1$ . The process is then applied to the  $(n - 1)$ -dimensional element  $(x - x_1)$  in  $R[x_1]$ , and we obtain a 1-dimensional element  $x_2$  such that  $\dim(x - x_1 - x_2) = n - 2$ . This process is done  $n$  times to obtain the desired sum. Moreover, if  $R$  is augmented, then each step can be taken to respect the augmentation.

Here is the exact statement of the result.

**Theorem 1.44 (The Splitting Principle).** *Let  $x$  be an  $n$ -dimensional element in a  $\lambda$ -ring  $R$ . Then there exists a  $\lambda$ -ring  $S$  containing  $R$  such that*

$$x = x_1 + \cdots + x_n$$

*in  $S$ , in which each  $x_i$  is 1-dimensional. Moreover, if  $R$  is augmented with  $\varepsilon(x) = m$ , then the augmentation can be extended to  $S$  in such a way that*

$$\varepsilon(x_r) = \begin{cases} 1 & \text{if } 1 \leq r \leq m, \\ 0 & \text{if } m < r \leq n. \end{cases}$$

In order to prove this Theorem, we need some preliminary results.

**Lemma 1.45.** *The polynomial  $P_{n,m}$  (Example 1.7) satisfies*

$$P_{n,m}(s_1, \dots, s_{m-1}, 0, \dots, 0) = 0. \tag{1.17}$$

*Therefore, every non-zero term in  $P_{n,m}(s_1, \dots, s_{nm})$  contains a factor of  $s_i$  for some  $i \geq m$ .*

**Proof.** Recall that  $P_{n,m}$  is the polynomial with integer coefficients in  $nm$  variables such that the coefficient of  $t^n$  in

$$g(t) = \prod_{1 \leq i_1 < \cdots < i_m \leq nm} (1 + x_{i_1} \cdots x_{i_m} t)$$

is  $P_{n,m}(s_1, \dots, s_{nm})$ , where  $s_i$  is the  $i$ th elementary symmetric function in the  $x_j$ 's. Setting  $x_m = x_{m+1} = \cdots = x_{nm} = 0$  in  $g$ , it follows that the coefficient of  $t^n$  is 0. This proves (1.17). □

**Lemma 1.46.** *Let  $R$  be a  $\lambda$ -ring, and let  $x$  be an  $n$ -dimensional element in  $R$ . Let  $y$  be a variable. In the polynomial  $\lambda$ -ring  $R[y]$  in which  $y$  has dimension one (Proposition 1.34), the ideal  $I$  generated by the element*

$$z = y^n - \lambda^1(x)y^{n-1} + \cdots + (-1)^{n-1}\lambda^{n-1}(x)y + (-1)^n\lambda^n(x)$$

*is a  $\lambda$ -ideal.*

**Proof.** By Proposition 1.28, it suffices to show that  $\lambda^m(z) \in I$  for  $m \geq 1$ . To do this, we first claim that  $I$  is also generated by  $\lambda^n(x - y)$ . Indeed, one has

$$\begin{aligned} \lambda_t(x - y) &= \lambda_t(x)\lambda_t(y)^{-1} && \text{(by Proposition 1.13)} \\ &= (1 + \lambda^1(x)t + \dots + \lambda^n(x)t^n)(1 + yt)^{-1} \\ &= (1 + \lambda^1(x)t + \dots + \lambda^n(x)t^n)(1 - yt + y^2t^2 - \dots). \end{aligned}$$

For  $r \geq 0$ , the coefficients of  $t^{n+r}$  yield the equality

$$\begin{aligned} \lambda^{n+r}(x - y) &= (-1)^{n+r}y^r (y^n - \lambda^1(x)y^{n-1} + \dots + (-1)^n\lambda^n(x)) \\ &= (-1)^{n+r}y^r z. \end{aligned} \tag{1.18}$$

Setting  $r = 0$  we see that  $z = (-1)^n\lambda^n(x - y)$ , so  $I$  is also generated by  $\lambda^n(x - y)$ .

To prove the Lemma, it suffices to show that  $\lambda^m(\lambda^n(x - y)) \in I$  for  $m \geq 1$ . Now

$$\lambda^m(\lambda^n(x - y)) = P_{m,n}(\lambda^1(x - y), \dots, \lambda^{mn}(x - y))$$

is a sum of terms, each one containing a factor of  $\lambda^{n+r}(x - y)$  for some  $r \geq 0$  (by Lemma 1.45). Since  $\lambda^{n+r}(x - y) \in I$  by (1.18), we conclude that  $\lambda^m(\lambda^n(x - y)) \in I$  as well.  $\square$

**Lemma 1.47.** *In the setting of Theorem 1.44, there exists a  $\lambda$ -ring  $R[x_1]$  containing  $R$  such that  $\dim(x_1) = 1$  and  $\dim(x - x_1) = n - 1$ . Moreover, if  $R$  is augmented with  $\varepsilon(x) = m$ , then the augmentation can be extended to  $R[x_1]$  in such a way that*

$$\varepsilon(x_1) = \begin{cases} 1 & \text{if } m > 0, \\ 0 & \text{if } m = 0. \end{cases}$$

*In particular, one has*

$$\varepsilon(x - x_1) = \begin{cases} m - 1 & \text{if } m > 0, \\ 0 & \text{if } m = 0. \end{cases}$$

**Proof.** Consider the quotient  $\lambda$ -ring  $R[x_1] = R[y]/I$ , in which  $y$  and  $I$  are as in Lemma 1.46 and  $x_1$  is the image of  $y$  in the quotient. The element  $x_1$  has dimension 1 because  $y$  does. Moreover, the element  $(x - x_1)$  has dimension  $(n - 1)$  because  $\lambda^{n+r}(x - y) \in I$  for  $r \geq 0$  by (1.18) and  $\lambda^{n-1}(x - y) \notin I$

Now suppose that  $R$  is augmented. Recall that the  $\lambda$ -ring  $R[y]$  can be augmented by either  $\varepsilon(y) = 0$  or  $\varepsilon(y) = 1$  by Proposition 1.34. If  $\varepsilon(I) = 0$ , then  $R[x_1]$  is augmented by  $\varepsilon(w + I) = \varepsilon(w)$  for  $w \in R[y]$ . If  $\varepsilon(x) = m$ , then

$$\varepsilon(\lambda^r(x)) = \lambda^r(\varepsilon(x)) = \binom{m}{r}.$$

Now if  $m > 0$ , we augment  $R[y]$  by setting  $\varepsilon(y) = 1$ . This implies that

$$\begin{aligned} \varepsilon(z) &= \varepsilon(y^n - \lambda^1(x)y^{n-1} + \dots + (-1)^{n-1}\lambda^{n-1}(x)y + (-1)^n\lambda^n(x)) \\ &= 1 - \binom{m}{1} + \binom{m}{2} + \dots + (-1)^m \binom{m}{m} \\ &= (1 - 1)^m \\ &= 0. \end{aligned}$$

The second equality uses the fact that  $\varepsilon(x) = m \leq n = \dim(x)$  (by Proposition 1.33). Therefore,  $\varepsilon(I) = 0$ , and we can augment  $R[x_1]$  by setting  $\varepsilon(x_1) = \varepsilon(y) = 1$ .

On the other hand, if  $m = 0$ , then we augment  $R[y]$  by setting  $\varepsilon(y) = 0$ . This implies that

$$\begin{aligned} \varepsilon(z) &= \varepsilon(y^n - \lambda^1(x)y^{n-1} + \dots + (-1)^{n-1}\lambda^{n-1}(x)y + (-1)^n\lambda^n(x)) \\ &= 0. \end{aligned}$$

Since  $\varepsilon(I) = 0$ , we obtain the induced augmentation  $\varepsilon(x_1) = \varepsilon(y) = 0$  on  $R[x_1]$ .  $\square$

**Proof.** [Proof of Theorem 1.44] Perform a downward induction on  $n = \dim(x)$  using Lemma 1.47. We obtain a  $\lambda$ -ring  $S = R[x_1, \dots, x_n]$  in which each  $x_i$  has dimension 1 and  $(x - x_1 - \dots - x_n)$  has dimension 0, i.e.,  $x = x_1 + \dots + x_n$ , as desired.  $\square$

**Corollary 1.48.** *Let  $x$  be an  $n$ -dimensional element in a  $\lambda$ -ring  $R$ . Then  $\lambda^n(x)$  is 1-dimensional.*

**Proof.** Extending  $R$  to  $S$  if necessary as in Theorem 1.44, we can write  $x$  as the sum of  $n$  one-dimensional elements  $x_i$  ( $1 \leq i \leq n$ ). Then

$$\begin{aligned} \lambda^n(x) &= \lambda^n(x_1 + \dots + x_n) \\ &= x_1 \cdots x_n, \end{aligned}$$

which is 1-dimensional because each  $x_i$  is (Proposition 1.13 (6)).  $\square$

### 1.6 Exercises

- (1) Let  $f(t) = 1 + t + a_2t^2 + a_3t^3 + \dots$  be a power series with integer coefficients. Show that  $\lambda_t(n) = f(t)^n$  defines a pre- $\lambda$ -ring structure on  $\mathbf{Z}$ .
- (2) Prove Theorem 1.8.
- (3) Write the coefficient of  $t^k$  ( $2 \leq k \leq 5$ ) in

$$g(t) = \prod_{1 \leq i < j \leq 4} (1 + x_i x_j t)$$

as a polynomial in the elementary symmetric functions on  $x_1, x_2, x_3, x_4$ . See Example 1.7.

- (4) Write down the polynomials  $P_{2,3}$  and  $P_{3,2}$  (Example 1.7) explicitly.
- (5) Write down the polynomials  $P_3$  and  $P_4$  (Example 1.9) explicitly.
- (6) Prove that  $P_n(a_1, \dots, a_n; b_1, \dots, b_n)$  is a polynomial in which every non-zero monomial contains a factor of  $a_i$  and a factor of  $b_j$  for some  $i, j \in \{1, \dots, n\}$ .
- (7) Let  $s_1, \dots, s_n$  be the elementary symmetric functions of the variables  $x_1, \dots, x_n$ . Prove:
  - (a) Each  $x_i^n$  lies in the ideal  $\langle s_1, \dots, s_n \rangle$  generated by  $s_1, \dots, s_n$  in the polynomial ring  $\mathbf{Z}[x_1, \dots, x_n]$ .

- (b) Let  $f \in \mathbf{Z}[x_1, \dots, x_n]$  be a homogeneous polynomial of degree  $> n(n-1)$ . Then  $f$  lies in the ideal  $\langle s_1, \dots, s_n \rangle$ .
- (8) Finish the proof of Proposition 1.13.
- (9) Prove Proposition 1.27.
- (10) Check that the map  $p_{r+1}: \Omega_{r+1} \rightarrow \Omega_r$  in (1.10) is actually a  $\lambda$ -homomorphism.
- (11) Modify the constructions in §1.3 to construct the free  $\lambda$ -ring  $U_2$  on two generators  $s_1$  and  $\sigma_1$ . Show that it has the right universal property, analogous to Theorem 1.39.
- (12) Define a natural operation  $\mu$  with two inputs on  $\lambda$ -rings as a rule that assigns to every  $\lambda$ -ring  $R$  a function  $\mu_R: R \times R \rightarrow R$  that is natural with respect to  $\lambda$ -homomorphisms. Write down the exact definition. Then prove the analogue of The Verification Principle (Theorem 1.43) for such operations.