11 The symmetric algebra

Throughout this section let $(R, +, \cdot)$ always be a commutative ring with a multiplicative identity element, and let M be an R-module.

11.1 Definition. Let $p \in \mathbb{N}_{>0}$, and let N be an R-module. A p-linear map $\varphi : M^p \to N$ is called *symmetric*, if for all $\sigma \in \Sigma_p$ holds

$$\varphi \circ \sigma \;=\; \varphi.$$

11.2 Notation. The R-module of symmetric p-linear maps is denoted by

$$\mathrm{Sym}^p_R(M, N) \;:=\; \{\varphi : M^p \to N :\; \varphi \text{ symmetric}\}$$

We define a submodule of the of the R-module $\bigotimes^p M$ by

$$Y^p(M) \;:=\; \mathrm{span}_R \left\{t - \tau(t) :\; t \in \textstyle\bigotimes^p M,\; \tau \in \Sigma_p \text{ transposition}\right\}.$$

11.3 Remark. a) Let $t \in \bigotimes^p M$, and let $\sigma \in \Sigma_p$ be an arbitrary permutation. Then $t - \sigma(t) \in Y^p(M)$. Indeed, we can write $\sigma = \tau_1 \circ \ldots \circ \tau_n$ as a composition of finitely many transpositions. We compute inductively

$$\begin{aligned} t - \sigma(t) \;&=\; (t - \tau_n(t)) + (\tau_n(t) - \tau_{n-1} \circ \tau_n(t)) + \ldots \\ &\quad \ldots + (\tau_2 \circ \ldots \circ \tau_n(t) - \tau_1 \circ \tau_2 \circ \ldots \circ \tau_n(t)) \;\in\; Y^p(M). \end{aligned}$$

b) The submodule $Y^p(M)$ is Σ_p-invariant. Indeed, let $\sigma \in \Sigma_p$. Then for any generating element $t - \tau(t) \in Y^p(M)$, with $t \in \bigotimes^p M$ and a transposition $\tau \in \Sigma_p$, we have $\sigma(t - \tau(t)) = \sigma(t) - \sigma \circ \tau \circ \sigma^{-1}(\sigma(t))$, which is an element of $Y^p(M)$ by **a)**.

11.4 Definition. Let M be an R-module, and let $p \in \mathbb{N}_{>0}$. The R-module quotient

$$S^p M \;:=\; \textstyle\bigotimes^p M / Y^p(M)$$

is called the *p-th symmetric product of* M. For equivalence classes, we use the notation

$$m_1 \vee \ldots \vee m_p := [m_1 \otimes \ldots \otimes m_p] \in S^p M.$$

Any element of $S^p M$, which can be written in this way, shall be called *decomposable*. The canonical quotient map of the p-th symmetric product is written on decomposable elements as

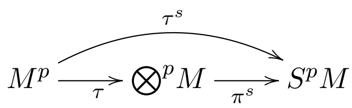
$$\begin{array}{rccc} \pi^s : & \bigotimes^p M & \to & S^p M \\ & m_1 \otimes \ldots \otimes m_p & \mapsto & m_1 \vee \ldots \vee m_p \end{array}$$

By the construction of the p-th symmetric product as a quotient, we clearly have

$$S^p M = \operatorname{span}_R \{m_1 \vee \ldots \vee m_p : (m_1, \ldots, m_p) \in M^p\}.$$

The rules for adding and multiplying elements in $S^p M$ are analogous to those for elements in $\bigotimes^p M$.

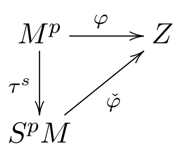
11.5 Remark. Note that the composed map τ^s, defined as the composition



is p-linear and symmetric. Indeed, let $m = (m_1, \ldots, m_p) \in M^p$, and let $\sigma \in \Sigma_p$ be a permutation. By remark 11.3, we have in $\bigotimes^p M$ the inclusion $m_1 \otimes \ldots \otimes m_p - \sigma(m_1 \otimes \ldots \otimes m_p) \in Y^p(M)$. Hence $\tau^s(m) - \tau^s \circ \sigma(m) = 0 \in S^p M$, as claimed.

11.6 Proposition. *Let M be an R-module, and let $p \in \mathbb{N}_{>0}$. The p-th symmetric power of M is up to isomorphism uniquely characterized by the following universal property.*

For any R-module Z, and any symmetric p-linear map $\varphi : M^p \to Z$, there exists a unique R-linear map $\check{\varphi}$ such that the diagram



commutes.

Proof. Compare proposition **??**. □

11.7 Remark. As before, we obtain a functor

$$\begin{array}{rccc} S^p: & (R\text{-Mod}) & \to & (R\text{-Mod}) \\ & M & \mapsto & S^p M \\ & \alpha & \mapsto & S^p \alpha \end{array}$$

where for any homomorphism $\alpha : M \to M'$ of R-modules and for all generating elements $m_1 \vee \ldots \vee m_p \in S^p M$ holds

$$S^p \alpha(m_1 \vee \ldots \vee m_p) = \alpha(m_1) \vee \ldots \vee \alpha(m_p) \in S^p M'.$$

11.8 Proposition. *Let M be a free R-module of rank $n < \infty$. Let $p \in \mathbb{N}_{>0}$. Then S^pM is a free R-module of rank*

$$\mathrm{rank}(S^pM) \;=\; \binom{n+p-1}{p}.$$

Proof. Let $\{e_i\}_{i=1,\dots,e_n}$ be a basis of M. By construction, S^pM is generated by $(e_{i_1} \vee \dots \vee e_{i_p})_{1 \le i_1,\dots,i_p \le n}$. Using the symmetry property , it is enough to consider ordered indices, so that $\{e_{i_1} \vee \dots \vee e_{i_p}\}_{1 \le i_1 \le \dots \le i_p \le n}$ is a generating family. It is easy combinatorics to see that this family has $\binom{n+p-1}{p}$ members, so that $\mathrm{rank}(S^pM) \le \binom{n+p-1}{p}$. A standard proof shows the linear independence, so that $\{e_{i_1} \vee \dots \vee e_{i_p}\}_{1 \le i_1 \le \dots \le i_p \le n}$ is indeed a basis. □

11.9 Example. Let M be a free R-module with a finite basis $\{e_i\}_{i=1,\dots,n}$. Let $p \in \mathbb{N}_{>0}$. Consider the ring of polynomials $R[X_1, \dots, X_n]$ as an R-module. The submodule of *homogeneous polynomials of degree* p is given by

$$R_p[X_1, \dots, X_n] := \mathrm{span}_R\{X_1^{d_1} \cdot \ldots \cdot X_n^{d_n} : d_1, \dots, d_n \in \mathbb{N},\, d_1 + \dots + d_n = p\}.$$

We define a p-linear map by

$$\begin{array}{cccc} \varphi_p : & M^p & \to & R_p[X_1, \dots, X_n] \\ & (m_1, \dots, m_p) & \mapsto & (\sum_{j=1}^n r_{1,j}X_j) \cdot \ldots \cdot (\sum_{j=1}^n r_{p,j}X_j) \end{array}$$

where for any $i = 1, \dots, p$ the element $m_i \in M$ is written with respect to the basis as R-linear combination $m_i = r_{i,1}e_1 + \dots + r_{i,n}e_n$. Since the ring of polynomials is commutative, the map φ_p is symmetric. By the universal property of the p-th symmetric product, there exists a unique R-linear map $\check{\varphi}_p : S^pM \to R[X_1, \dots, X_n]$ such that for all decomposable elements $m_1 \vee \dots \vee m_p \in S^pM$ holds

$$\check{\varphi}_p(m_1 \vee \dots \vee m_p) = \varphi_p(m_1, \dots, m_p).$$

In particular, for any $1 \le i_1, \dots, i_p \le n$ holds $X_{i_1} \cdot \ldots \cdot X_{i_p} = \check{\varphi}_p(e_{i_1} \vee \dots \vee e_{i_p})$, which implies, that the map $\check{\varphi}_p$ is surjective. One easily computes

$$\mathrm{rang}(R_p[X_1, \dots, X_n]) \;=\; \binom{n+p-1}{p}.$$

Together with our arguments from the proof of proposition 11.8, we find that $\check{\varphi}_p$ is an isomorphism of free R-modules

$$S^pM \;\cong\; R_p[X_1, \dots, X_n].$$

Note that the direct sum $R[X_1, \ldots, X_n] = \bigoplus_{p\in\mathbb{N}} R_d[X_1, \ldots, X_n]$ is more than just an R-module: it has even the structure of an R-algebra. This motivates the following definition.

11.10 Definition. Let M be an R-module. The *symmetric algebra of M* is given as an R-module by

$$SM \;:=\; \bigoplus_{p\in\mathbb{N}} S^p M,$$

where $S^0 M := R$.

11.11 Remark. As before, one shows that there exists a unique R-algebra structure "$\vee$" on SM, such that the direct sum $\pi^s : \bigotimes M \to SM$ of the canonical quotient maps is a homomorphism of R-algebras.

In particular, if $a \in S^p M$ and $a' \in S^q M$ are given as $a = \pi^s(t)$ and $a' = \pi^s(t')$ for some $t \in \bigotimes^p M$ and $t' \in \bigotimes^q M$, then their algebra product equals

$$a \vee a' \;=\; \pi^s(t \otimes t').$$

11.12 Proposition. *Let M be an R-module. Then its symmetric algebra SM is a graded commutative R-algebra with multiplicative unit 1_R.*

Proof. Straightforward. □

11.13 Proposition. *Let M be a free R-module of rank $n < \infty$. Then there exists an isomorphism of R-algebras*

$$SM \;\cong\; R[X_1, \ldots, X_n].$$

Proof. For the underlying isomorphism of R-modules see example 11.9. We leave it as an exercise to verify its compatibility with the respective algebra multiplications. □

11.14 Remark. Let L, M, N be free R-modules such that $M = N \oplus L$. Then there exists an isomorphism of graded R-algebras

$$SM \;\cong\; SN \otimes SL.$$

In particular, for all $k \in \mathbb{N}$ holds

$$S^k M \;\cong\; \bigoplus_{p+q=k} S^p N \otimes S^q L.$$

12 Derivations and differentials

An important application of tensor products in general, and alternating products in particular, is found in differential geometry and in physics: the theory of differentials is essential for advanced calculus. We want to illustrate this in one elementary example.

Throughout this section let $(R, +, \cdot)$ always be a commutative ring with a multiplicative identity element. Let $(A, +, \lambda, \sigma)$ be a commutative and associative R-algebra with a unital element 1_A. In particular, $(A, +, \sigma)$ is a commutative ring with a multiplicative identity element. Let M be an A-module, an thus an R-module, too.

12.1 Definition. An R-linear map $D : A \to M$ is called a *derivation*, if it satisfies for all $a, b \in A$ the *Leibniz rule*:

$$D(ab) = aD(b) + bD(a).$$

12.2 Remark. We denote by $\mathrm{Der}_R(A, M)$ the set of all derivations from A to M. It is a submodule of the R-module $\mathrm{Hom}_R(A, M)$.

12.3 Example. Let $I \subset \mathbb{R}$ be an open interval of real numbers. For a natural number $n \in \mathbb{N}$, let $C^n(I)$ denote the set of all n-times continuously differentiable functions $f : I \to \mathbb{R}$. Note that $C^n(I)$ has the structure of a commutative and associative $\mathbb{R}$-algebra, where "+" and "·" are defined point-wise. The constant function 1 is a unital element in $C^n(I)$.

Moreover, for $f \in C^{n+1}(I)$ and $g \in C^n(I)$ holds $f \cdot g \in C^n(I)$. In this way, $M := C^n(I)$ becomes a module over $A := C^{n+1}(I)$. Consider the map

$$\begin{array}{rccc} D: & C^{n+1}(I) & \to & C^n(I) \\ & f & \mapsto & \frac{\partial f}{\partial x}. \end{array}$$

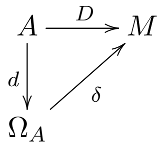
Clearly, differentiation is $\mathbb{R}$-linear, and it satisfies the product rule. Thus D is a derivation.

12.4 Lemma. *Let $D : A \to M$ be a derivation. Then $D(1_A) = 0_M$.*

Proof. From the Leibniz rule, we compute for the unital element $D(1_A) = D(1_A \cdot 1_A) = 1_A \cdot D(1_A) + 1_A \cdot D(1_A)$, and thus $D(1_A) = 0_M$. □

12.5 Definition. Let Ω_A be an A-module. A derivation $d : A \to \Omega_A$ is called a *universal derivation*, if it satisfies the following *universal property*:

For any A-module M, and any derivation $D : A \to M$, there exists a unique homomorphism of A-modules $\delta : \Omega_A \to M$, such that the diagram



commutes.

12.6 Fact. Universal derivations exist, and they are uniquely determined up to isomorphisms. Moreover, for any universal derivation $d : A \to \Omega_A$ holds $\Omega_A = \mathrm{span}_A\{d(a) : a \in A\}$.

12.7 Example. Consider the algebra of polynomials $k[x]$ over a field k. Let $d : k[x] \to \Omega_{k[x]}$ denote a universal derivation.

As a module over k, a generating family for $k[x]$ is given by $\{x^n\}_{n\in\mathbb{N}}$. By lemma 12.4, for $n = 0$ holds $d(x^0) = 0$. For $n \geq 2$, we compute inductively

$$d(x^n) = x^{n-1}d(x) + xd(x^{n-1}) = \ldots = n \cdot x^{n-1}d(x).$$

Using the $\mathbb{R}$-linearity of d, we obtain for any $f \in k[x]$ the formula

$$d(f) = \frac{\partial f}{\partial x}\, d(x),$$

where $\frac{\partial f}{\partial x}$ denotes the *formal* differentiation of a polynomial. This implies the equality $\mathrm{span}_{k[x]}\{d(f) : f \in k[x]\} = k[x] \cdot d(x)$. Therefore by 12.6, the $k[x]$-module $\Omega_{k[x]}$ is free of rank 1. A basis element is given by $dx := d(x)$, and we may write

$$\Omega_{k[x]} = k[x]\, dx.$$

12.8 Notation. Let $d : A \to \Omega_A$ be a universal derivation. We call Ω_A the A-module of *Kähler differentials*. For $p \in \mathbb{N}_{\geq 2}$ we write

$$\Omega^p_A := \bigwedge\nolimits^p \Omega_A$$

together with $\Omega^0_A := A$ and $\Omega^1_A := \Omega_A$.

12.9 Fact. There exists a family of R-linear maps $d_p : \Omega_A^p \to \Omega_A^{p+1}$ for $p \in \mathbb{N}$ such that for all $p, q \in \mathbb{N}$, all $\omega \in \Omega_A^p$ and all $\eta \in \Omega_A^q$ holds $d_{p+1} \circ d_p = 0$, and

$$d_{p+q}(\omega \wedge \eta) = d_p\omega \wedge \eta + (-1)^p \omega \wedge d_q\eta \quad \in \Omega_A^{p+q}.$$

The family $\{d_p\}_{p\in\mathbb{N}}$ is called the *de Rham complex* of Ω_A.

12.10 Example. Consider the ring of polynomials $A := \mathbb{R}[x, y, z]$ as an $\mathbb{R}$-algebra. Similarly to example 12.7 one obtains for the module of Kähler differentials Ω_A a free A-module of rank 3, with basis $\{dx, dy, dz\}$.

Because p-th exterior powers of Ω_A vanish for $p > 3$, the de Rham complex can be written as

$$\Omega_A^0 \xrightarrow{d_0} \Omega_A^1 \xrightarrow{d_1} \Omega_A^2 \xrightarrow{d_2} \Omega_A^3 \to 0.$$

Let us compute this maps explicitly for all $p = 0, 1, 2$. For $p = 0$, the $\mathbb{R}$-linear map $d_0 : \Omega_A^0 \to \Omega_A^1$ is just the universal derivation. One can show this to be the map

$$\begin{array}{rccc} d: & A & \to & \Omega_A \\ & f & \mapsto & \frac{\partial f}{\partial x}\, dx + \frac{\partial f}{\partial y}\, dy + \frac{\partial f}{\partial z}\, dz. \end{array}$$

In coordinates, i.e. with respect to the basis $\{dx, dy, dz\}$ of Ω_A^1 this map can be written as

$$d_0(f) = \begin{pmatrix} \frac{\partial f}{\partial x} \\ \frac{\partial f}{\partial y} \\ \frac{\partial f}{\partial z} \end{pmatrix} =: \mathbf{grad}(f).$$

In other words, the evaluation of universal derivation in some $f \in A$ is given by the *gradient* of f. For $d_1 : \Omega_A^1 \to \Omega_A^2$ one computes for a general element $fdx + gdy + hdz \in \Omega_A^1$ using the formulae from 12.9

$$\begin{aligned} d_1(fdx + gdy + hdz) &= d_1(fdx) + d_1(gdy) + d_1(hdz) \\ &= (df \wedge dx + (-1)^0 f \wedge d_1\, dg) + \ldots \\ &= df \wedge dx + dg \wedge dy + dh \wedge dz \\ &= (\tfrac{\partial f}{\partial x} dx + \tfrac{\partial f}{\partial y} dy + \tfrac{\partial f}{\partial z} dz) \wedge dx + \ldots \\ &= (-\tfrac{\partial f}{\partial y} + \tfrac{\partial g}{\partial x}) dx \wedge dy + \ldots \end{aligned}$$

We leave it to the reader to fill in the dots. It gets more readable when we use the notation in coordinates with respect to the bases $\{dx, dy, dz\}$ of Ω_A^1

and $\{dy \wedge dz, dz \wedge dx, dx \wedge dy\}$ of Ω^2_A:

$$d_1 \begin{pmatrix} f \\ g \\ h \end{pmatrix} = \begin{pmatrix} -\frac{\partial g}{\partial z} + \frac{\partial h}{\partial y} \\ \frac{\partial f}{\partial z} - \frac{\partial h}{\partial x} \\ -\frac{\partial f}{\partial y} + \frac{\partial g}{\partial x} \end{pmatrix} =: \mathbf{rot} \begin{pmatrix} f \\ g \\ h \end{pmatrix}.$$

This is known as the *rotation* of the triple of functions (f, g, h). Analogously, we obtain for $d_2 : \Omega^2_A \to \Omega^3_A$ for a general element

$$\begin{aligned} d_2(f dy \wedge dz + g dz \wedge dx + h dx \wedge dy) &= \\ &= df \wedge dy \wedge dz + dg \wedge dz \wedge dx + dh \wedge dx \wedge dy \\ &= (\tfrac{\partial f}{\partial x} dx + \tfrac{\partial f}{\partial y} dy + \tfrac{\partial f}{\partial z} dz) \wedge dy \wedge dz + \ldots \\ &= (\tfrac{\partial f}{\partial x} + \tfrac{\partial f}{\partial y} + \tfrac{\partial f}{\partial z}) dx \wedge dy \wedge dz. \end{aligned}$$

With respect to the bases $\{dy \wedge dz, dz \wedge dx, dx \wedge dy\}$ of Ω^2_A and $\{dx \wedge dy \wedge dz\}$ of Ω^3_A we get

$$d_2 \begin{pmatrix} f \\ g \\ h \end{pmatrix} = \frac{\partial f}{\partial x} + \frac{\partial f}{\partial y} + \frac{\partial f}{\partial z} =: \mathbf{div} \begin{pmatrix} f \\ g \\ h \end{pmatrix}.$$

This is the definition of the *divergence* of the triple of functions (f, g, h).

12.11 Proposition. *The following identities hold:*

$$\begin{aligned} \mathbf{rot} \circ \mathbf{grad} &= 0 \\ \mathbf{div} \circ \mathbf{rot} &= 0. \end{aligned}$$

Proof. For the de Rham complex holds $d \circ d = 0$. □