Math 332 Winter 2023, Lecture 24: Monoid algebras

website: `https://www.cip.ifi.lmu.de/~grinberg/t/23wa`

3. Monoid algebras and polynomials

Recall: For this entire chapter, we fix a **commutative** ring R.

3.1. Monoid algebras (cont'd)

Recall from Lecture 23: If M is any monoid (written multiplicatively), then $R[M]$ denotes the **monoid algebra** of M over R. This is the R-algebra that consists of all formal R-linear combinations $\sum\limits_{m\in M} r_m e_m$ of elements e_m with $m \in M$. So, as an R-module, it is just the free R-module

$$R^{(M)} = \left\{ (r_m)_{m\in M} \in R^M \ \mid \ \text{all but finitely many } m \in M \text{ satisfy } r_m = 0 \right\},$$

and the elements e_m are just the vectors that the standard basis of this free R-module $R^{(M)}$ comprises[1]. Its multiplication is the unique R-bilinear map from $R^{(M)} \times R^{(M)}$ to $R^{(M)}$ that satisfies

$$e_m e_n = e_{mn} \qquad \text{for all } m, n \in M.$$

Its unity is e_1, where 1 is the neutral element of M.

3.1.2. Examples (cont'd)

Last time, we began to analyze the monoid algebra (aka group algebra) $\mathbb{Q}[C_2]$, where C_2 is the cyclic group of order 2 (given as $C_2 = \{1, u\}$ where $u^2 = 1$).

The elements of this $\mathbb{Q}$-algebra $\mathbb{Q}[C_2]$ have the form $ae_1 + be_u$ where $a, b \in \mathbb{Q}$. They are multiplied according to the rule

$$(ae_1 + be_u)(ce_1 + de_u) = (ac + bd)e_1 + (ad + bc)e_u$$

(for $a, b, c, d \in \mathbb{Q}$). This makes it clear that the ring $\mathbb{Q}[C_2]$ is commutative.

I explained that $\mathbb{Q}[C_2]$ is not a field, and instead has zero-divisors:

$$(e_1 + e_u)(e_1 - e_u) = \underbrace{e_1^2}_{\substack{=e_1e_1 \\ =e_{1\cdot 1}=e_1}} - \underbrace{e_u^2}_{\substack{=e_ue_u \\ =e_{uu}=e_1}} = e_1 - e_1 = 0.$$

[1] Specifically, for each $m \in M$, the vector e_m is the m-th standard basis vector, i.e., the family $(\delta_{m,n})_{n\in M}$ that has a 1 in its m-th position and 0s in all other positions. It is the natural generalization of the standard basis vectors $(0, 0, \ldots, 0, 1, 0, 0, \ldots, 0)$ of an R-module R^n (but is more abstract due to the fact that the elements of an arbitrary monoid M do not come with a given order, and M can be infinite).

Note that e_1 is the unity of the algebra $\mathbb{Q}[C_2]$, so we can write 1 for it. Thus, $ae_1 + be_u$ becomes $a + be_u$.

I teased you with the claim that

$$\mathbb{Q}[C_2] \cong \mathbb{Q} \times \mathbb{Q} \qquad \text{as } \mathbb{Q}\text{-algebras.}$$

Let me quickly explain why this is true:

Recall that any central idempotent element of a ring R breaks this ring R into a direct product (Exercise 1 **(d)** on homework set #4). Thus, we want to find a central idempotent element of $\mathbb{Q}[C_2]$.

Here is one: Set $z := \frac{1}{2} + \frac{1}{2}e_u \in \mathbb{Q}[C_2]$. Then,

$$\begin{aligned} z^2 &= \left(\frac{1}{2} + \frac{1}{2}e_u\right)^2 = \frac{1}{4} + \frac{1}{2} \cdot \frac{1}{2}e_u + \frac{1}{2}e_u \cdot \frac{1}{2} + \frac{1}{4}\underbrace{e_u^2}_{=1} \\ &= \frac{1}{4} + \frac{1}{4}e_u + \frac{1}{4}e_u + \frac{1}{4} = \frac{1}{2} + \frac{1}{2}e_u = z. \end{aligned}$$

Thus, z is idempotent. Since $\mathbb{Q}[C_2]$ is commutative, this z is furthermore central. Hence, by the above-mentioned exercise, we obtain

$$\mathbb{Q}[C_2] \cong z\mathbb{Q}[C_2] \times (1-z)\mathbb{Q}[C_2]$$

(as rings, but by the same logic as $\mathbb{Q}$-algebras as well[2]). Now, I claim that both $\mathbb{Q}$-algebras $z\mathbb{Q}[C_2]$ and $(1-z)\mathbb{Q}[C_2]$ are isomorphic to $\mathbb{Q}$. Indeed, for $z\mathbb{Q}[C_2]$, this follows easily from the fact that

$$\begin{aligned} z \cdot (a + be_u) &= \left(\frac{1}{2} + \frac{1}{2}e_u\right) \cdot (a + be_u) \\ &= \left(\frac{1}{2}a + \frac{1}{2}b\right) + \left(\frac{1}{2}b + \frac{1}{2}a\right) e_u \\ &= \frac{a+b}{2} + \frac{a+b}{2}e_u = (a+b)\, z \qquad \text{for all } a, b \in \mathbb{Q}. \end{aligned}$$

For $(1-z)\mathbb{Q}[C_2]$, this is similar (notice that $1 - z = \frac{1}{2} - \frac{1}{2}e_u$). With a bit of work, this leads to the $\mathbb{Q}$-algebra isomorphism

$$\begin{aligned} g : \mathbb{Q}[C_2] &\to \mathbb{Q}^2, \\ a + be_u &\mapsto (a+b,\ a-b) \qquad \text{(for all } a, b \in \mathbb{Q}\text{)} \end{aligned}$$

(where $\mathbb{Q}^2$ means the direct product $\mathbb{Q} \times \mathbb{Q}$ of $\mathbb{Q}$-algebras).

A few more remarks:

[2] To be more precise: If we fix a commutative ring S and replace the word "ring" by "S-algebra" throughout Exercise 1 on homework set #4, then the exercise remains true, and the solution does not get much harder (there are some more straightforward axioms to be verified).

- There is an obvious reason why $\mathbb{Q}[C_2] \cong \mathbb{Q}^2$ as $\mathbb{Q}$-modules: Indeed, $\mathbb{Q}[C_2]$ has a basis (e_1, e_u) that consists of two vectors, so we can obtain a $\mathbb{Q}$-module isomorphism $f : \mathbb{Q}[C_2] \to \mathbb{Q}^2$ by mapping $e_1 \mapsto (1, 0)$ and $e_u \mapsto (0, 1)$. Explicitly, this isomorphism f sends each $a + be_u$ to (a, b). But this is **not** a $\mathbb{Q}$-algebra isomorphism (e.g., because $e_1 e_u$ is nonzero but $(1, 0)(0, 1)$ is zero). Our above $\mathbb{Q}$-algebra isomorphism $g : \mathbb{Q}[C_2] \to \mathbb{Q}^2$ is more sophisticated.

- We can easily repeat the above explorations of $\mathbb{Q}[C_2]$ using $\mathbb{R}$ or $\mathbb{C}$ instead of $\mathbb{Q}$.

  However, things change if we try to repeat them using $\mathbb{Z}$. Indeed, the idempotent element $z = \frac{1}{2} + \frac{1}{2}e_u$ does not exist over $\mathbb{Z}$ because $\frac{1}{2} \notin \mathbb{Z}$. Thus, the group algebra $\mathbb{Z}[C_2]$ has no reason to be isomorphic to $\mathbb{Z}^2$. And indeed, it is not. (For a proof, see Example 4.1.5 **(b)** in the text.)

Here is another example of a monoid ring:

Example 3.1.1. Consider the cyclic group $C_3 = \{1, u, v\}$ of order 3 with $u^3 = 1$ and $u^2 = v$. Its group algebra $\mathbb{Q}[C_3]$ has a central idempotent

$$z := \frac{1 + e_u + e_v}{3}.$$

More generally, for any finite group G, the group algebra $\mathbb{Q}[G]$ has a central idempotent

$$z := \frac{\sum\limits_{g \in G} e_g}{|G|}.$$

(Exercise: Prove this!) The principal ideal $z\mathbb{Q}[G]$ is always $\cong \mathbb{Q}$ as a $\mathbb{Q}$-algebra. Thus, using Exercise 1 **(d)** on homework set #4 (extended from rings to algebras), we obtain

$$\mathbb{Q}[G] \cong \mathbb{Q} \times S \qquad \text{(as } \mathbb{Q}\text{-algebras)},$$

where $S = (1 - z)\mathbb{Q}[G]$. In the case $G = C_2$, we found $S \cong \mathbb{Q}$, but in the general case S can be more complicated.

3.1.3. General properties of monoid algebras

Let us now discuss some general properties of and conventions on monoid algebras.

Proposition 3.1.2. Let M be an **abelian** monoid. Then, the monoid ring $R[M]$ is commutative.

Proof. See the text (Proposition 4.1.9). This is again a proof "by linearity". □

Proposition 3.1.3. Let M be a monoid with neutral element 1. Then, the map

$$\begin{aligned} R &\to R[M], \\ r &\mapsto r \cdot e_1 \end{aligned}$$

is an injective R-algebra morphism.

Proof. See the text (Proposition 4.1.10). Injectivity is clear; morphicity relies on $e_1 e_1 = e_1$. □

Convention 3.1.4. If M is a monoid, then we shall identify each $r \in R$ with $r \cdot e_1 \in R[M]$. This identification is harmless (i.e., does not lead to false conclusions)[3], and turns R into an R-subalgebra of $R[M]$.

An element of $R[M]$ will be called **constant** if it lies in this subalgebra (i.e., if it is $r \cdot e_1$ for some $r \in R$).

Warning: We previously explained that $\mathbb{Q}[C_2] \cong \mathbb{Q} \times \mathbb{Q}$ as $\mathbb{Q}$-algebras. Now we have identified $\mathbb{Q}$ with a subalgebra of $\mathbb{Q}[C_2]$. But this subalgebra is not one of the two $\mathbb{Q}$ factors in $\mathbb{Q}[C_2] \cong \mathbb{Q} \times \mathbb{Q}$; in fact, none of those two $\mathbb{Q}$ factors is a $\mathbb{Q}$-subalgebra. Our $\mathbb{Q}$-algebra isomorphism from $\mathbb{Q}[C_2]$ to $\mathbb{Q} \times \mathbb{Q}$ sends the unity of $\mathbb{Q}[C_2]$ to $(1,1) \in \mathbb{Q} \times \mathbb{Q}$, which does not lie completely in either factor.

Proposition 3.1.5. Let M be a monoid. Then, the map

$$\begin{aligned} M &\to R[M], \\ m &\mapsto e_m \end{aligned}$$

is a monoid morphism from M to $(R[M], \cdot, 1)$.

Proof. This is just saying that $e_{mn} = e_m e_n$ and $e_1 = 1_{R[M]}$. Both hold by definition of $R[M]$. □

Our last two propositions tell us that the monoid algebra $R[M]$ "includes" both R and M in an appropriate way (at least when R is nontrivial). Thus, we can view it as what comes out if we "throw" the elements of M into R.

This suggests another convention:

Convention 3.1.6. Let M be a monoid. Then, the elements e_m of the standard basis $(e_m)_{m \in M}$ of $R[M]$ will just be written as m if there is no confusion to worry about.

For example, if M is the cyclic group C_3 as above, then the element $ae_1 + be_u + ce_v$ will just be written as $a1 + bu + cv = a + bu + cv$.

[3] This follows from Proposition 3.1.3.

For another example, if M is the cyclic group C_2 as above, then our multiplication rule

$$(ae_1 + be_u)(ce_1 + de_u) = (ac + bd) e_1 + (ad + bc) e_u$$

(for $a, b, c, d \in R$) rewrites as

$$(a + bu)(c + du) = (ac + bd) + (ad + bc) u.$$

3.2. Polynomial rings

3.2.1. Univariate polynomials

We can now effortlessly define univariate polynomials: They are just elements of certain monoid algebras. Which ones?

Recall that R denotes a commutative ring. Recall also that $\mathbb{N} = \{0, 1, 2, \ldots\}$.

Definition 3.2.1. Let C be the free monoid with a single generator x. This is the monoid whose elements are countably many distinct symbols called

$$x^0, \quad x^1, \quad x^2, \quad x^3, \quad \ldots,$$

and whose operation is defined by

$$x^i \cdot x^j = x^{i+j} \qquad \text{for all } i, j \in \mathbb{N}.$$

Of course, this monoid is just the well-known additive monoid $(\mathbb{N}, +, 0)$ in a multiplicative disguise (with each nonnegative integer i renamed as x^i in order to avoid overloading the notation $i \cdot j$).

The neutral element of this monoid C is x^0. We set $x := x^1$.

The elements of C are called **monomials** in the variable x. The specific element x is called the **indeterminate**.

Now, the **univariate polynomial ring** $R[x]$ over R is defined to be the monoid algebra $R[C]$. Following Convention 3.1.6, we simply write m for the standard basis vector e_m when $m \in C$. That is, we write x^i for the basis vector e_{x^i}. Thus, $R[x]$ is a free R-module with basis

$$\left(x^0, x^1, x^2, x^3, \ldots\right) = \left(1, x, x^2, x^3, \ldots\right).$$

Hence, any $p \in R[x]$ can be written as a finite R-linear combination of powers of x. That is, p can be written as

$$p = a_0 x^0 + a_1 x^1 + a_2 x^2 + \cdots + a_n x^n = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

for some $n \in \mathbb{N}$ and some $a_0, a_1, \ldots, a_n \in R$. This representation is unique up to trailing zeroes (i.e., up to adding extra terms of the form $0x^{n+1}$ and $0x^{n+2}$ and so on).

Elements of $R[x]$ are called **polynomials** in x over R.

Thus, up to notation, the univariate polynomial ring $R[x]$ is just the monoid ring $R[\mathbb{N}]$ of the abelian monoid $\mathbb{N} = (\mathbb{N}, +, 0)$. Hence, it is commutative (since $\mathbb{N}$ is abelian).

Example 3.2.2. **(a)** The sum

$$1 + 3x^2 + 6x^3 = 1e_{x^0} + 3e_{x^2} + 6e_{x^3}$$

belongs to $R[x]$, i.e., is a polynomial in x.

(b) The infinite sum

$$1 + x + x^2 + x^3 + \cdots$$

is **not** a polynomial, because it is not a **finite** R-linear combination of powers of x (unless R is trivial). We defined the polynomial ring $R[x]$ to be $R[C]$, so that it is $R^{(C)}$ as an R-module (not R^C). Infinite sums like $1 + x + x^2 + \cdots$ would make sense in R^C and are known as **formal power series**, but they are not polynomials; they are a subject of their own.

So we have defined **univariate** polynomial rings (i.e., polynomial rings in a single variable). Likewise, we can define **multivariate** polynomial rings (i.e., polynomial rings in several variables). For simplicity, let me restrict myself to finitely many variables.

3.2.2. Multivariate polynomials

Definition 3.2.3. Let $n \in \mathbb{N}$. Let $C^{(n)}$ be the free abelian monoid with n generators $x_1, x_2, \ldots, x_n$. This is the monoid whose elements are the distinct symbols

$$x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \qquad \text{with } i_1, i_2, \ldots, i_n \in \mathbb{N},$$

and whose operation is given by

$$\left(x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}\right)\left(x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}\right) = x_1^{i_1+j_1} x_2^{i_2+j_2} \cdots x_n^{i_n+j_n}.$$

If we wrote this monoid additively, it would just be $\mathbb{N}^n$ (the additive monoid of n-tuples of nonnegative integers, with entrywise addition), but we write it multiplicatively.

The elements of $C^{(n)}$ are called **monomials**.

For each $i \in \{1, 2, \ldots, n\}$, the monomial

$$x_1^0 x_2^0 \cdots x_{i-1}^0 x_i^1 x_{i+1}^0 x_{i+2}^0 \cdots x_n^0$$

will be denoted by x_i. These specific monomials $x_1, x_2, \ldots, x_n$ are called the **indeterminates**.

Now, the R-algebra $R[x_1, x_2, \ldots, x_n]$ is defined to be the monoid algebra $R\left[C^{(n)}\right]$. It is called the **polynomial ring in n variables $x_1, x_2, \ldots, x_n$ over R**. Any element of this R-algebra can be written as an R-linear combination

$$\sum_{(i_1, i_2, \ldots, i_n) \in \mathbb{N}^n} r_{i_1, i_2, \ldots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

with $r_{i_1, i_2, \ldots, i_n} \in R$ (such that all but finitely many of these coefficients $r_{i_1, i_2, \ldots, i_n}$ are 0).

Elements of $R[x_1, x_2, \ldots, x_n]$ are called **polynomials** in $x_1, x_2, \ldots, x_n$.

For example, for $R = \mathbb{Z}$, the sum

$$4x_1^2 + x_2 x_3 + 7x_3^5 - 3$$

is a polynomial in $x_1, x_2, \ldots, x_n$ whenever $n \geq 3$. For $R = \mathbb{R}$, the sums

$$3x_1 + 14x_1 x_2^3 \qquad \text{and} \qquad \sqrt{2} x_1^7 - \frac{3}{2} x_1^3 x_2 + \pi$$

are polynomials in $x_1, x_2, \ldots, x_n$ whenever $n \geq 2$. You can easily construct examples like this ad infinitum.

Note that the univariate polynomial ring $R[x]$ is just the particular case of the polynomial ring $R[x_1, x_2, \ldots, x_n]$ in n variables $x_1, x_2, \ldots, x_n$ obtained by setting $n = 1$ and renaming the indeterminate x_1 as x.