§1.3: ALGEBRAS

DEFINITION: Let A be a ring. An **A-algebra** is a ring R equipped with a ring homomorphism $\phi : A \to R$; we call ϕ the **structure morphism** of the algebra[1]. A **homomorphism** of A-algebras is a ring homomorphism that is compatible with the structure morphisms; i.e., if $\phi : A \to R$ and $\psi : A \to S$ are A-algebras, then $\alpha : R \to S$ is an A-algebra homomorphism if $\alpha \circ \phi = \psi$.

UNIVERSAL PROPERTY OF POLYNOMIAL RINGS: Let[2] A be a ring, and $T = A[X_1, \ldots, X_n]$ be a polynomial ring. For any A-algebra R, and any collection of elements $r_1, \ldots, r_n \in R$, there is a unique A-algebra homomorphism $\alpha : T \to R$ such that $\alpha(X_i) = r_i$.

DEFINITION: Let A be a ring, and R be an A-algebra. Let S be a subset of R. The **subalgebra generated by** S, denoted $A[S]$, is the smallest A-subalgebra of R containing S.

DEFINITION: Let R be an A-algebra. Let $r_1, \ldots, r_n \in R$. The ideal of **A-algebraic relations** on $r_1, \ldots, r_n$ is the set of polynomials $f(X_1, \ldots, X_n) \in A[X_1, \ldots, X_n]$ such that $f(r_1, \ldots, r_n) = 0$ in R. Equivalently, the ideal of A-algebraic relations on $r_1, \ldots, r_n$ is the kernel of the homomorphism $\alpha : A[X_1, \ldots, X_n] \to R$ given by $\alpha(X_i) = r_i$. We say that a set of elements in an A-algebra is **algebraically independent over** A if it has no nonzero A-algebraic relations.

DEFINITION: A **presentation** of an A-algebra R consists of a set of generators $r_1, \ldots, r_n$ of R as an A-algebra and a set of generators $f_1, \ldots, f_m \in A[X_1, \ldots, X_n]$ for the ideal of A-algebraic relations on $r_1, \ldots, r_n$. We call $f_1, \ldots, f_m$ a set of **defining relations** for R as an A-algebra.

PROPOSITION: If R is an A-algebra, and $f_1, \ldots, f_m$ is a set of defining relations for R as an A-algebra, then $R \cong A[X_1, \ldots, X_n]/(f_1, \ldots, f_m)$.

(1) Let R be an A-algebra and $r_1, \ldots, r_n \in R$.
- **(a)** Explain why $A[r_1, \ldots, r_n]$ is the image of the A-algebra homomorphism $\alpha : A[X_1, \ldots, X_n] \to R$ such that $\alpha(X_i) = r_i$.
- **(b)** Discuss the following: $A[r_1, \ldots, r_n]$ is the set of elements of R that can be written as "polynomial expressions in $r_1, \ldots, r_n$ with coefficients from $\phi(A)$" (if the structure map is ϕ).
- **(c)** Suppose that $R = A[r_1, \ldots, r_n]$ and let $f_1, \ldots, f_m$ be a set of generators for the kernel of the map α. Explain why $R \cong A[X_1, \ldots, X_n]/(f_1, \ldots, f_m)$, i.e., why the Proposition above is true.
- **(d)** Suppose that R is generated as an A-algebra by a set S. Let I be an ideal of R. Explain why R/I is generated as an A-algebra by the image of S in R/I.
- **(e)** Let $R = A[X_1, \ldots, X_n]/(f_1, \ldots, f_m)$, where $A[X_1, \ldots, X_n]$ is a polynomial ring over A. Find a presentation for R.

- **(a)** Clearly $\mathrm{im}(\alpha) \subseteq R$ is an A-subalgebra that contains $r_1, \ldots, r_n$, so $A[r_1, \ldots, r_n] \subseteq \mathrm{im}(\alpha)$. On the other hand, since $r_1, \ldots, r_n \in A[r_1, \ldots, r_n]$, we have $\alpha(X_i) \in A[r_1, \ldots, r_n]$, so we can consider α as an A-algebra homomorphism from $A[X_1, \ldots, X_n] \to A[r_1, \ldots, r_n]$, and hence $\mathrm{im}(\alpha) \subseteq A[r_1, \ldots, r_n]$.
- **(b)** This is just another way of thinking about $\mathrm{im}(\alpha)$: $\alpha(\sum a_i X_1^{i_1} \cdots X_n^{i_n}) = \sum \phi(a_i) r_1^{i_1} \cdots r_n^{i_n}$.
- **(c)** This is just the First Isomorphism Theorem applied along with (a).

[2]Note: the same R with different ϕ's yield different A-algebras. Despite this we often say "Let R be an A-algebra" without naming the structure morphism.

[2]This is equally valid for polynomial rings in infinitely many variables $T = A[X_\lambda \mid \lambda \in \Lambda]$ with a tuple of elements of $\{r_\lambda\}_{\lambda \in \Lambda}$ in R in bijection with the variable set. I just wrote this with finitely many variables to keep the notation for getting too overwhelming.

(d) If $K[\{X_\lambda\}] \to R$ where the variables map to the elements of S is surjective, then composing with the quotient map gives a surjection $K[\{X_\lambda\}] \to R \to R/I$ where the variables map to the images of elements of S.

(e) R is generated by $[X_1], \ldots, [X_n]$, with defining relations $f_1, \ldots, f_m$.

(2) Presentations of some subrings:

(a) Consider the $\mathbb{Z}$-subalgebra of $\mathbb{C}$ generated by $\sqrt{2}$. Write the notation for this ring. Is there a more compact description of the set of elements in this ring? Find a presentation.

(b) Same as (a) with $\sqrt[3]{2}$ instead of $\sqrt{2}$.

(c) Let K be a field, and $T = K[X, Y]$. Come up with a concrete description of the ring $R = K[X^2, XY, Y^2] \subseteq T$, (i.e., describe in simple terms which polynomials are elements of R), and give a presentation as a K-algebra.

(a) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \cong \mathbb{Z}[X]/(X^2 - 2)$

(b) $\mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Z}\} \cong \mathbb{Z}[X]/(X^3 - 2)$.

(c) $K[X^2, XY, Y^2]$ is the collection of polynomials that only have even degree terms. We computed the kernel of the presenting map last time, in slightly different words and letters, and saw that the kernel is generated by $X_2^2 - X_1X_3$.

(3) Infinitely generated algebras:

(a) Show that $\mathbb{Q} = \mathbb{Z}[1/p \mid p \text{ is a prime number}]$.

(b) True or false: It is a direct consequence of the conclusion of (a) and the fact that there are infinitely many primes that $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}$-algebra.

(c) Given $p_1, \ldots, p_m$ prime numbers, describe the elements of $\mathbb{Z}[1/p_1, \ldots, 1/p_m]$ in terms of their prime factorizations. Can you ever have $\mathbb{Z}[1/p_1, \ldots, 1/p_m] = \mathbb{Q}$ for a finite set of primes?

(d) Show that $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}$-algebra.

(e) Show that, for a field K, the algebra $K[X, XY, XY^2, XY^3, \ldots] \subseteq K[X, Y]$ is not a finitely generated K-algebra.

(f) Show that, for a field K, the algebra $K[X, Y/X, Y/X^2, Y/X^3, \ldots] \subseteq K(X, Y)$ is not a finitely generated K-algebra.

(a) The $\supseteq$ containment is clear. For the other, take $a/b \in \mathbb{Q}$, and write $b = p_1^{e_1} \cdots, p_n^{e_n}$. Then $a/b = a(1/p_1)^{e_1} \cdots (1/p^n)^{e_n}$ exhibits a/b in the right hand side.

(b) False! There could be a different finite generating set.

(c) An element of $\mathbb{Z}[1/p_1, \ldots, 1/p_m]$ can be written as $\sum_\alpha a_\alpha (1/p_1)^{\alpha_1} \cdots (1/p_m)^{\alpha_m}$ so has a denominator that is a product of powers of p_i's. This can never equal $\mathbb{Q}$, since $1/(p_1 \cdots p_m + 1)$ can't be written in this form: if so, and in lowest terms with numerator a, after clearing denominators we would have $p_1^{\alpha_1} \cdots p_n^{\alpha_n} = (p_1 \cdots p_m + 1)a$, which contradicts the expression in lowest terms.

(d) If $\mathbb{Q} = \mathbb{Z}[a_1/b_1, \ldots, a_n/b_n]$ (in lowest terms) let $p_1, \ldots, p_m$ be the prime factors of $b_1, \ldots, b_n$. Then $\mathbb{Z}[a_1/b_1, \ldots, a_n/b_n] \subseteq \mathbb{Z}[1/p_1, \ldots, 1/p_m]$, so $\mathbb{Z}[1/p_1, \ldots, 1/p_m] = \mathbb{Q}$ contradicting what we just showed.

(e) Suppose otherwise that $K[X, XY, XY^2, XY^3, \ldots] = K[f_1, \ldots, f_n]$. Since each f_i is a polynomial expression of $X, XY, XY^2, XY^3, \ldots$, and there are finitely many XY^j that appear in (fixed expressions for) each of the finitely many f_i, we have $K[X, XY, XY^2, XY^3, \ldots] \subseteq K[f_1, \ldots, f_n] \subseteq K[X, XY, \ldots, XY^m]$ for some m, and equality holds for this same m. We claim that $XY^{m+1} \notin K[X, XY, \ldots, XY^m]$, which will yield the desired contradiction. Indeed, one can see that every monomial in $K[X, XY, \ldots, XY^m]$ has its y-exponent is less

than or equal to m times its x-exponent, which is not true of XY^{m+1}. This is the desired contradiction.

(f) Similar to the previous.

(4) Give two different nonisomorphic $\mathbb{C}[X]$-algebra structures on $\mathbb{C}$.

We can write $\mathbb{C} \cong \mathbb{C}[X]/(X)$ or $\mathbb{C} \cong \mathbb{C}[X]/(X-1)$, for example. These are not isomorphic as $\mathbb{C}[X]$-algebras, since such a morphism would send $[0]$ to $[0]$ and $[X]$ to $[X]$, but $[X] = [0]$ in $\mathbb{C}[X]/(X)$ while $[X] = [1]$ in $\mathbb{C}[X]/(X-1)$.

(5) Let K be a field. Describe which elements are in the K-algebra $K[X, X^{-1}] \subseteq K(X)$, and find an element of $K(X)$ not in $K[X, X^{-1}]$. Then compute[3] a presentation for $K[X, X^{-1}]$ as a K-algebra.

The elements of $K[X, X^{-1}]$ are rational functions that can be written with a power of X as a denominator. The rational function $1/(X-1)$ is not in this algebra.

We claim that $K[X, X^{-1}] \cong K[X_1, X_2]/(X_1X_2 - 1)$. Clearly $X_1X_2 - 1$ is a relation on X and X^{-1}. If it does not generate, take a relation not in the ideal among which has lowest X_2-degree. Let $f(X_1, X_2) = f_n(X_1)X_2^n + f_{n-1}(X_1)X_2^{n-1} + \cdots + f_0(X_1)$ be an algebraic relation, and consider the top X_2-degree coefficient $f_n(X_1)$ of f. Note that f_n is a multiple of X_1 since, mapping $X_1 \mapsto X$ and $X_2 \mapsto X^{-1}$, we get $f_n(X)X^{-n} + f_{n-1}(X)X^{-n+1} + \cdots + f_0(X) = 0$, so $f_n(X) = X(-f_{n-1}(X) - Xf_{n-2}(X) - \cdots - X^n f_0(X))$. Write $f_n = X_1 f_n'$. Then

$$\begin{aligned} f(X_1, X_2) &= f_n(X_1)X_2^n + f_{n-1}(X_1)X_2^{n-1} + \cdots + f_0(X_1) \\ &= X_1 f_n'(X_1)X_2^n + f_{n-1}(X_1)X_2^{n-1} + \cdots + f_0(X_1) \\ &= (X_1X_2 - 1)f_n'(X_1)X_2^{n-1} + (f_n'(X_1) + f_{n-1})X_2^{n-1} + \cdots + f_0(X_1). \end{aligned}$$

Subtracting off a multiple of $X_1X_2 - 1$, we obtain a relation of lower X_2-degree, contradicting the choice of our relation, and hence the existence of a relation that is not a multiple of $X_1X_2 - 1$.

(6) Let K be a field, and $T = K[X, Y]$. Let $R \subseteq T$ be the ring of polynomials that only have terms whose degree is a multiple of three (e.g., $X^3 + \pi X^5 Y + 5$ is in while $X^3 + \pi X^4 Y + 5$ is out). Show that R is generated by X^3, X^2Y, XY^2, Y^3, with defining relations $X_2^2 - X_1X_3, X_3^2 - X_2X_4, X_1X_4 - X_2X_3$.

Since $X^3, X^2Y, XY^2, Y^3 \in R$, we have $K[X^3, X^2Y, XY^2, Y^3] \subseteq R$. To show equality, note that we can write $f \in R$ as a sum of monomials of degree a multiple of three, so it suffices to show that any such monomial is in the algebra generated by X^3, X^2Y, XY^2, Y^3. Given X^iY^j, if $i \geq 3$ or $j \geq 3$, we can write $X^iY^j = X^3\mu$ or $Y^3\mu$ with μ a smaller monomial of degree a multiple of three. Continuing like so, we can assume $i, j < 3$, in which case we must have X^2Y or XY^2. Thus, $K[X^3, X^2Y, XY^2, Y^3] = R$.

Now we compute the ideal of relations. We can check directly that each relation is in the defining ideal. To see that they generate, we show that any polynomial in the kernel of the presenting map is equivalent to zero modulo the ideal generated by the given three. Write $T = X_1, U = X_2, V = X_3, W = Y^3$. Given a relation F, we think of it as a polynomial in V. We can use division via $V^2 - UW$ to get rid of the $V^{\geq 2}$ terms, and the other relations to rewrite the coefficient of the V^1 term as a polynomial in W alone, so $F \equiv f_1(W)V + f_0(T, U, W)$. Then we have $f_1(Y^3)XY^2 + f_0(X^3, X^2Y, Y^3) = 0$. The first term only produces Y^1-terms, while the second produces only other powers of Y, so the two parts must be zero. This implies that f_1 is the zero

[3] Hint: Note that Division does not apply. Say $X_1 \mapsto X$ and $X_2 \mapsto Y$. Show that the top X_2-degree coefficient of an algebraic relation is a multiple of X_1, and use this to set an induction on the top X_2-degree.

polynomial, and that f_0 is a relation on X^3, X^2Y, Y^3. A similar division argument shows that any polynomial in T, U, W that vanishes upon mapping $T \mapsto X^3$, $U \mapsto X^2Y$, $W \mapsto Y^3$ is a multiple of $U^3 - T^2W$, but $U^3 - T^2W = U(U^2 - TV) - T(TW - UV)$. This completes the proof.

(7) Jacobian criterion for algebraic independence: Let K be a field of characteristic zero, $R = K[X_1, \ldots, X_n]$ be a polynomial ring, and $f_1, \ldots, f_n \in R$ be n polynomials. Show that $f_1, \ldots, f_n$ are algebraically independent over K if and only if

$$\det \begin{bmatrix} \frac{\partial f_1}{\partial X_1} & \cdots & \frac{\partial f_n}{\partial X_1} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_1}{\partial X_n} & \cdots & \frac{\partial f_n}{\partial X_n} \end{bmatrix} \neq 0.$$

Use this to show that the 2×2 minors of a 2×3 matrix of indeterminates are algebraically independent.