WHAT IS A POLYNOMIAL?

1. A Construction of the Complex Number Field

Take the real number field $\mathbb{R}$ as given. The vector space $\mathbb{R}^2$ over $\mathbb{R}$ carries the algebraic operations of addition and scalar multiplication. With no explanation, one can also define multiplication on $\mathbb{R}^2$ by the rule

$$(x,y)(x',y') = (xx' - yy', xy' + x'y).$$

And then one can verify, although the verification is tedious in places, that

- The newly-defined algebraic structure $(\mathbb{R}^2, +, \cdot)$ is a field.
- The map
$$\mathbb{R} \longrightarrow \mathbb{R}^2, \quad x \longmapsto (x,0)$$
is an injective homomorphism of fields.
- If, in light of the previous bullet, we identify $\mathbb{R}$ with the subfield $\mathbb{R} \times \{0\}$ of $\mathbb{R}^2$, then the elements
$$(0, \pm 1) \in \mathbb{R}^2$$
are square roots of -1.
- If we call those two elements $\pm i$ and let $\mathbb{C}$ be a new name of the field $\mathbb{R}^2$ then
$$\mathbb{C} = \{x + iy : x, y \in \mathbb{R}\}.$$

This process *constructs* the familiar description of the complex number field without invoking square roots of -1. Of course, this construction is not the first way that a person would conceive of the complex number field.

The field $\mathbb{C} = \mathbb{R}^2$ visibly forms a 2-dimensional vector space over $\mathbb{R}$. Although the above construction of $\mathbb{C}$ may appear ad hoc, what is easier to show is that *any* field that forms a 2-dimensional vector space over $\mathbb{R}$ is field-isomorphic to $\mathbb{C}$. Thus any peculiarities of the construction of $\mathbb{C}$ are irrelevant.

This handout discusses polynomial algebras in terms similar to this introductory example of the complex number field.

Let R be a commutative ring with 1. From experience, we think of a polynomial over R as an expression of the form

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

where X is an *indeterminate*, and n is a nonnegative integer, and each $a_i \in R$, and $a_n \neq 0$. (The description precludes 0, so it needs to be admitted as a polynomial as well.) And any value may be substituted for X.

But these ideas raise questions. Is the primitive notion of an indeterminate any more sensible than the primitive notion of a square root of -1? Is it any more necessary? In what sense of *any* can any value be substituted for X? Are there other algebraic objects that are effectively the same thing as polynomials?

In addressing these questions, the key ideas are as follows.

- We describe the totality of polynomials having coefficients in R as an algebraic structure. The structure in question is a commutative *R-algebra*, meaning an associative, commutative ring A having scalar multiplication by R. (From now on in this writeup, algebras are understood to be commutative.)
- The algebraic structure is not described by internal details of what its elements are, but rather by how it interacts with other R-algebras. Specifically, the description takes the form of a *characteristic mapping property.*
- The mapping property quickly shows that the internal details of the polynomial algebra over R are unique up to isomorphism, so that how we go about describing them doesn't particularly matter, although we do have to describe them one way or another in order to show that the polynomial algebra over R exists at all.
- The mapping property of the polynomial algebra can be decisively more useful than the internal description.

2. Definition and Uniqueness of the Polynomial Algebra

The idea of the polynomial algebra allowing the unique substitution of any value for the indeterminate is captured by the following definition.

Definition 2.1. *The polynomial algebra over R is an R-algebra $\mathcal{P}$ containing a distinguished element X such that*

> *For any R-algebra A and any element $\alpha \in A$, there is a unique R-algebra homomorphism*
>
> $$\mathcal{P} \longrightarrow A$$
>
> *such that*
>
> $$X \longmapsto \alpha.$$

The definition refers to *the* polynomial algebra over R with no explanation of whether such a thing exists or is unique. In fact, uniqueness is wired into the definition.

Proposition 2.2. *Suppose that $\mathcal{P}$ and $\mathcal{Q}$ are polynomial algebras over R, having distinguished elements X and Y. Then there is a unique R-algebra isomorphism*

$$\mathcal{P} \longrightarrow \mathcal{Q}$$

such that

$$X \longmapsto Y.$$

Proof. Since $\mathcal{P}$ and $\mathcal{Q}$ are both polynomial algebras over R, the definition says that there are unique R-algebra homomorphisms

$$\varphi : \mathcal{P} \longrightarrow \mathcal{Q}, \quad X \longmapsto Y$$

and

$$\psi : \mathcal{Q} \longrightarrow \mathcal{P}, \quad Y \longmapsto X.$$

We want to show that φ is an isomorphism.

The composition

$$\psi \circ \varphi : \mathcal{P} \longrightarrow \mathcal{P}, \quad X \longmapsto X$$

is an R-algebra homomorphism. But the definition says that there is a *unique* such R-algebra homomorphism, and certainly the identity map on $\mathcal{P}$ fits the bill. Thus $\psi \circ \varphi$ is the identity map on $\mathcal{P}$. Similarly, $\varphi \circ \psi$ is the identity map on $\mathcal{Q}$. □

Thus there is at most one polynomial algebra over R. And so, whatever the details of any actual construction of the polynomial algebra (and the construction must work with fully-understood notions, avoiding reference to an *indeterminate*), the end-result will always be the same. But we still don't know that a polynomial algebra over R exists at all.

3. A Construction of the Polynomial Algebra

As one construction of the polynomial algebra over R, take

$$\mathcal{P} = \{\text{sequences } (a_n)_{n\geq 0} \text{ in } R \text{ such that } a_n = 0 \text{ for all } n \gg 0\}.$$

That is, a polynomial is a sequence with only finitely many nonzero terms,

$$(a_0, a_1, a_2, \cdots, a_n, 0, 0, 0, \cdots).$$

It is clear how to add such sequences and how to scale such a sequence by an element of R,

$$(a_n) + (b_n) = (a_n + b_n), \qquad r(a_n) = (ra_n).$$

Define the product of two such sequences to be

$$(a_n)(b_n) = (c_n) \quad \text{where } c_n = \sum_{j+k=n} a_j b_k.$$

The product operation is associative by a short calculation that

$$((a_n)(b_n))(c_n) = (\sum_{i+j+k=n} a_i b_j c_k) = (a_n)((b_n)(c_n)).$$

Then $(1, 0, 0, \cdots)$ is the multiplicative identity of $\mathcal{P}$, and also induction quickly shows that for all $n \geq 0$

$$(0, 1, 0, 0, \cdots)^n = (0, \cdots, 0, 1, 0, 0, \cdots) \quad \text{(with the 1 in the } n\text{th slot)}.$$

Thus if we define

$$X = (0, 1, 0, 0, \cdots)$$

then every element of $\mathcal{P}$ takes the form

$$(a_0, a_1, a_2, \cdots, a_n, 0, 0, \cdots) = a_0 \cdot 1_{\mathcal{P}} + a_1 X + a_2 X^2 + \cdots + a_n X^n,$$

and multiplication in $\mathcal{P}$ becomes, inevitably,

$$\big(\sum a_i X^i\big)\big(\sum b_j X^j\big) = \sum c_k X^k \quad \text{where } c_k = \sum_{i+j=k} a_i b_j.$$

Now, given any R-algebra A and any element $\alpha \in A$, the only possible R-algebra homomorphism

$$\mathcal{P} \longrightarrow A, \quad X \longmapsto \alpha$$

is the map

$$\varphi : a_0 \cdot 1_{\mathcal{P}} + a_1 X + a_2 X^2 + \cdots + a_n X^n \longmapsto a_0 \cdot 1_A + a_1 \alpha + a_2 \alpha^2 + \cdots + a_n \alpha^n.$$

The question is whether φ preserves products. It does, because the multiplication law in $\mathcal{P}$ gives

$$\begin{aligned}\varphi\big(\big(\sum a_i X^i\big)\big(\sum b_j X^j\big)\big) &= \varphi\big(\sum c_k X^k\big) \quad \text{where } c_k = \sum_{i+j=k} a_i b_j \\ &= \sum c_k \alpha^k,\end{aligned}$$

while multiplication in A gives

$$\begin{aligned}\varphi\big(\sum a_i X^i\big)\varphi\big(\sum b_j X^j\big) &= \big(\sum a_i \alpha^i\big)\big(\sum b_j \alpha^j\big) \\ &= \sum c_k \alpha^k \quad \text{where } c_k = \sum_{i+j=k} a_i b_j.\end{aligned}$$

4. An Example

Consider a nonzero irreducible polynomial $f(X) \in \mathbb{Q}[X]$. Let α and β be two complex roots of f. Consider the smallest superfield of $\mathbb{Q}$ containing α, and similarly for β,

$$k_\alpha = \mathbb{Q}(\alpha), \qquad k_\beta = \mathbb{Q}(\beta).$$

The question is,

Is the set-map that takes α to β and fixes $\mathbb{Q}$ pointwise,

$$k_\alpha \longrightarrow k_\beta, \quad \alpha \longmapsto \beta,$$

a field isomorphism?

It is not at all clear that the map should respect the algebra of the two fields, for example.

However, the polynomial ideal

$$I = \langle f(X) \rangle \subset \mathbb{Q}[X]$$

is the set of polynomials in $\mathbb{Q}[X]$ satisfied by α. To see this, first note that on the one hand, clearly $g(\alpha) = 0$ for all $g(X) \in I$. On the other hand, if $g(X) \in \mathbb{Q}[X]$ is not a multiple of $f(X)$ then the irreducibility of $f(X)$ means that $\gcd(f(X), g(X)) = 1$,

$$F(X)f(X) + G(X)g(X) = 1 \quad \text{for some } F(X), G(X) \in \mathbb{Q}[X].$$

Substitute α for X to get $G(\alpha)g(\alpha) = 1$, so that $g(\alpha) \neq 0$.

Thus the unique $\mathbb{Q}$-algebra homomorphism

$$\varphi_\alpha : \mathbb{Q}[X] \longrightarrow \mathbb{Q}[\alpha], \quad X \longmapsto \alpha$$

has kernel I, giving a $\mathbb{Q}$-algebra isomorphism

$$\overline{\varphi}_\alpha : \mathbb{Q}[X]/I \xrightarrow{\sim} \mathbb{Q}[\alpha], \quad X \longmapsto \alpha.$$

Similarly, we get a $\mathbb{Q}$-algebra isomorphism

$$\overline{\varphi}_\beta : \mathbb{Q}[X]/I \xrightarrow{\sim} \mathbb{Q}[\beta], \quad X \longmapsto \beta,$$

and thus a $\mathbb{Q}$-algebra isomorphism

$$\overline{\varphi}_\beta \circ \overline{\varphi}_\alpha^{-1} : \mathbb{Q}[\alpha] \xrightarrow{\sim} \mathbb{Q}[\beta], \quad \alpha \longmapsto \beta.$$

To finish the argument, observe that $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha) = k_\alpha$ and similarly for β. The point is that for any nonzero expression $g(\alpha) \in \mathbb{Q}[\alpha]$, the polynomial $g(X) \in \mathbb{Q}[X]$ is coprime to $f(X)$ as explained above, and consequently $G(\alpha)g(\alpha) = 1$ for some $G[X] \in \mathbb{Q}[X]$, also as explained above.