Constants, Variables, Polynomials, Functions

Given a group G and an element $g \in G$, what are the elements of G that are "automatically" created as a result? In other words, what elements do the *axioms* of a group guarantee for us.

Obviously, the identity element 1_G ($= g^0$!) is already there. Then we have the positive powers g^n of g. We also have the inverse g^{-1} of g and *its* powers g^{-n} for n a positive integer. In other words, we have a map $\mathbb{Z} \to G$. In fact, this is a homomorphism of groups.

Conversely, given a homomorphism $\mathbb{Z} \to G$, the image of 1 in G is an element g of G.

In summary, giving an element of G is the *same* as giving a homomorphism of groups $\mathbb{Z} \to G$. Is there something similar for rings?

Polynomials

Given a ring R and an element a in R, what are the elements of R that are automatically created? As above, we can form the positive powers a^n of a and the multiplicative identity 1 is already in R. Now we can *add* and *subtract* any (finite) number of copies of such elements to get elements like $1+1+1-a-a+a^3$ or equivalently $3-2\cdot a+a^3$. In other words, We can create elements of the form

$$n_0 + n_1 a + n_2 a^2 + \cdots + n_k a^k$$

where k is a non-negative integer and n_0, n_1, ... are integers.

Exercise: Check that the sum and product of two such elements is an element of the same type.

Hence, it is natural to introduce a *ring* that consists of elements of the form

$$n_0 + n_1 T + n_2 T^2 + \cdots + n_k T^k$$

where T is a *variable*. We define multiplication by the rule $T^a \cdot T^b = T^{a+b}$ and extend it by the distributive law. Addition is defined by collecting terms that have the same power of T. This collection gives us the ring $\mathbb{Z}[T]$ of *polynomials* in one variable T.

Exercise: Write down the formulas for addition and multiplication of a general pair of polynomials.

In particular, for any ring R we can *define* $R[T]$ to consist of "formal" expressions of the type $a_0 + a_1 T + \cdots + a_k T^k$ where we now allow a_i to be elements of R.

Multiplication and addition can be defined by the same formulas as in the above exercise. This is the polynomial ring over R.

We note that giving an element a of a ring R is the *same* as giving a ring homomorphism $\mathbb{Z}[T] \to R$. This homomorphism sends the variable T to the element a. Can we extend this idea to $R[T]$ in some way?

Constants

The integers are "constants" in a natural sense. We can expand the notion of constants. For example, we can multiply a $p \times p$ matrix M over a ring R by an element a of R. We do this by thinking of a as being the $p \times p$ matrix which has a along the diagonal and 0 outside. As seen before this gives a homomorphism $R \to M_p(R)$. This should be seen as an *extension* of the natural homomomorphism $\mathbb{Z} \to S$ for *any* ring S.

Given a commutative ring R and a ring homomorphism $f : R \to S$ such that $f(a) \cdot b = b \cdot f(a)$ for *any* element b of S. In this case we say that S is an *R-algebra* or that R is the ring of constants for S.

Why do we insist on the commutativity of R? The following exercise may help to understand. (This explanation is a little advanced and may be skipped at first reading!)

Exercise: (Starred) For a ring S and a fixed element s in S, define a map $D_s(a) = s \cdot a - a \cdot s$. This is *not* a ring homomorphism. However, check that $D_s(a+b) = D_s(a) + D_s(b)$ and (more importantly) $D_s(a \cdot b) = a \cdot D_s(b) + D_s(a) \cdot b$.

In other words, D_s behaves like differentiation and satisfies the Liebnitz rule. Now we would like our "constants" to have derivative 0. So we need $D_s(a) = 0$ for all s. Hence, constants need to commute with all elements of S.

A more elementary reason to take R to be commutative can be seen by the following exercise.

Exercise: Suppose that R is commutative and that S is an R-algebra. Show that giving an element of S is the same as giving a homomorphism $R[T] \to S$ where the map is the natural one on R.

On the other hand, we have the following:

Exercise: Suppose $a \cdot b \neq b \cdot a$ in R, then show that the map $R[T] \to R$ which sends T to a is *not* a homomorphism.

Functions

Given a ring R and a set A, the collection $\mathrm{Map}(A, R)$ is a ring in a natural way. Given functions $f : A \to R$ and $g : A \to R$ we define addition and multiplication "pointwise":

$$(f+g)(a) = f(a) + g(a) \text{ and } (f \cdot g)(a) = f(a) \cdot g(a)$$

The "constant" function $\underline{0}$ that takes the value 0 for all values of a plays the role of additive identity, while the "constant" function $\underline{1}$ that takes the value 1 for all values of a plays the role of multiplicative identity.

Exercise: Check that the above definitions make $\mathrm{Map}(A, R)$ into a ring.

In what follows we will take R to be a commutative ring.

Polynomials can be turned into functions as follows. Given a polynomial $p(T) = a_0 + a_1 T + \cdots a_k T^k$, we have the function e_p in $\mathrm{Map}(R, R)$ which sends an element b in R to

$$e_p(b) = a_0 + a_1 \cdot b + \cdots a_k \cdot b^k$$

This is usually called the *evaluation* of the polynomial at b.

Exercise: Check that evaluation gives a ring homomorphism $R[T] \to \mathrm{Map}(R, R)$.

Exercise: (Starred) Does the above statement hold if R is not commutative? Give an example to justify your answer.

One may be tempted to identify the notion of polynomials with functions which can be expressed as polynomials (the image of the above homomorphism). However, the following example shows why this is fallacious.

We take $R = \mathbb{Z}/2$. In this case $\mathrm{Map}(\mathbb{Z}/2, \mathbb{Z}/2)$ is just the collection of set maps from a 2 element set to a 2 element set. This has $2^2 = 4$ elements. On the other hand the ring $(\mathbb{Z}/2)$[T]$ of polynomials has the *infinite* collection of *distinct* elements $1, T, \ldots, T^k, \ldots$. Thus, the above ring homomorphism has a non-zero kernel.

In fact, we can see that $e_T(0) = 0$ and $e_T(1) = 1$; at the same time $e_{T^2}(0) = 0$ and $e_{T^2}(1) = 1$. Thus, $e_T = e_T^2$ and so $e_{T^2 - T} = 0$.

Exercise: How many elements are there in the set $\mathrm{Map}(\mathbb{Z}/n, \mathbb{Z}/n)$?

Exercise: For $n = 3, 4, 5, 6$, find an explicit polynomial $p(T)$ in $(\mathbb{Z}/n)[T]$ for which $e_p(k) = 0$ for *every* element k in $\mathbb{Z}/n$.

This can be generalised to the following.

Exercise: Find an explicit polynomial $p(T)$ in $(\mathbb{Z}/n)[T]$ for which $e_p(k) = 0$ for *every* element k in $\mathbb{Z}/n$.

In summary, polynomials give rise to functions, but there is more to polynomials than just the functions associated with them.