Lecture 7 FORMAL POWER SERIES.

Some algebraic systems we have experience with

Group : – assoc. / unity / inverse $(\mathbb{Z},+)$

Abelian group : – Commutative $\mathbb{Z}_m^*$

Ring : 2 operations + : Abelian Group ; · : Assoc. / unity ; Dist law $(\mathbb{Z},+,\cdot)$ $\mathbb{Z}_m$

(commutative with unity)

Field : 2 operations + : Abelian Group ; · : $\mathbb{F}\setminus\{0\}$ is abelian group ; dist. law — $\mathbb{Z}_p$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

We invent one more today. Let R be a ring and q be some symbol

$$R[[q]] := \left\{\sum_{i=0}^{\infty} a_i q^i = a_0 + a_1 q + a_2 q^2 + a_3 q^3 + \dots \;\middle|\; a_i \in R\right\}$$

$\sum a_i q^i \longleftrightarrow (a_0, a_1, a_2, a_3, \dots)$ ← infinite string.

Since we calculate only a finite # of them we use the symbol $O(q^n)$ to denote where we have calculated until.

Ex: $1+q+q^2+O(q^3)$ ← big O.

Def:

$=$: $a = \sum a_i q^i = \sum b_i q^i = b$ if $a_i = b_i$ for all i.

$+$: $a+b = \sum_{i=0}^{\infty} (a_i+b_i) q^i$ (a_i+b_i is defined in ring). add – assoc / comm / 0 / inverse

$\times$: $a \cdot b = \left(\sum a_i q^i\right)\left(\sum b_i q^i\right) := \sum_{i=0}^{\infty} c_i q^i$, where $c_n = a_n b_0 + a_{n-1} b_1 + \dots + a_0 b_n$

Example: $(0,1,0,0,\dots) \times (0,1,0,0,\dots) = (0,0,1,0,0,\dots)$

$c_0 = 0\cdot 0$

$c_1 = 1\cdot 0 + 0\cdot 1 = 0$

$c_2 = 0\cdot 0 + 1\cdot 1 + 0\cdot 0 = 1$

$c_3 = 0\cdot 0 + 1\cdot 0 + 0\cdot 1 + 0\cdot 0 = 0$

$q \leftrightarrow (0,1,0,0,\dots)$

$q^2 \leftrightarrow (0,0,1,0,0,\dots)$

props
- associative
- commutative
- $(1,0,0,\dots) = 1 + 0\cdot q + 0 q^2 + \dots$ is unity

Ex: Show $q^k \cdot q^l = q^{k+l}$ in this.

Third operation $\cdot : R \times R[q] \to R[q]$ scalar multiplication

$$c\,a(q) = \sum_{i=0}^{\infty} c a_i q^i \quad \text{for } c \in R.$$

- $(c_1 c_2) a(q) = c_1 (c_2 a(q))$
- Dist laws – $c(a(q)+b(q)) = c a(q) + c b(q)$ etc. $(c_1+c_2) a(q) = c_1 a + c_2 a$.
- $1\cdot a = a$

We say $(R[[q]], +, \text{scalar mult})$ is a MODULE

$(R[[q]], +, \times, \text{scalar})$ is an algebra.

If $R = \mathbb{F}$, a field, → vector space ← modules are called

the main object of study in Linear Algebra

- $R[[q]]$ ← Ring structure
- $R[q]$ ← Ring of polynomials $\sum_{i=0}^{n} a_i q^i$, $a_n \neq 0$, n = degree of poly. also algebra.

Usually we use $\mathbb{Z}[[q]]$ in combinatorics, on occasion $\mathbb{Q}$. (I will give ex on these.)

Ex: Sage: try R.<q> = PowerSeriesRing(ZZ) ← sets context

$(1+q)^2 = \dots$

$(1+q)^{100} = \dots + O(q^{20})$ ← Default calc.

Theorem: (Imp) $(1-q)^{-1} = 1 + q + q^2 + \dots$ (in FPS.)

Proof: Consider $(1-q)(1+q+q^2+\dots)$

Coeff of q^m : $1 + (-1)(1) = 0$ (for $m>0$) ← coeff of q^{m-1} in

coeff of q^0 : $1\cdot 1 = 1$.

So $(1-q)(1+q+\dots) = 1$. □

Prop: Let $a = \sum a_i q^i$. Then a has a multiplicative inverse if and only if a_0 is invertible in R.

Proof: Sp a is invertible. Let $b = \sum_{i=0}^{\infty} b_i q^i$ be the inverse then $ab = 1 \Rightarrow (a_0 + a_1 q + \dots)(b_0 + b_1 q + \dots) = 1$

$\Rightarrow a_0 b_0 = 1 \Rightarrow a_0$ is invertible in R.

Conversely, let a be given and let $b = \sum_{i=0}^{\infty} b_i q^i$. Consider the equation $ab = 1$

$\Rightarrow a_0 b_0 = 1 \Rightarrow b_0 = a_0^{-1}$

$a_0 b_1 + a_1 b_0 = 0 \to a_0, a_1, b_0$ known b_1 ✓

$a_0 b_2 + a_1 b_1 + a_2 b_0 = 0 \to b_2$ can be calculated

$a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0 = 0 \to b_3 \dots$

This is a 'triangular' system and can be solved.

Ex. Write an inductive proof that $b_0, b_1, \dots, b_n, \dots$ can be found from this system.

Remarks (1) $R = \mathbb{Z}$, a_0 is invertible iff $a_0 = \pm 1$.

(2) We can define $R[[x,y]]$ as $R[x][y]$ etc. Same for $R[x,y]$ ← polynomials in 2 variables

(3) Can think of calculating inverses as follows:

$$\frac{1}{1+a_1 q + a_2 q^2 + \dots} = 1 - (a_1 q + a_2 q^2 + \dots)^1 + (a_1 q + a_2 q^2 + \dots)^2 + \dots$$

Can compute coeffts of q^m for $m = 0, 1, 2, \dots$ from here.

Def: Let $a(q) = \sum a_i q^i$. The formal derivative is defined as

$$D(a(q)) := \sum_{k=1}^{\infty} k a_k q^{k-1}.$$

Remarks (1) Can prove usual rules for diff from here.

(2) D^k is defined by iteration. $D^2 = D(D a)$ etc.

(3) if $D a(q) = 0 \Rightarrow k a_k = 0$ for $k \geq 1$

$\Rightarrow a_k = 0$ for $k \geq 1$

so $a(q) = a_0 + 0q + 0q^2 + \dots = a_0$.

(4)
$$\exp(x) = e^x := \sum_{k=0}^{\infty} \frac{x^k}{k!}$$

$$D(e^x) = \sum_{k=0}^{\infty} \frac{k x^{k-1}}{k!} = \sum_{k=1}^{\infty} \frac{x^{k-1}}{(k-1)!}$$

$$= e^x.$$

e ← meaningless here, but we still use it.

Prop: (Taylor expansion) $a = \sum a_k q^k$

$$a(q) = a_0 + D(a(0))\,q + D^2 a(0) \frac{q^2}{2!} + \dots$$

Here if $b(q) = \sum b_i q^i$, $b(0) = b_0$.

Proof: Ex (induction).

Remark: Sp $b(0) = 0$ then $a(b(q)) = \sum_{i=0}^{\infty} a_i (b(q))^i$ makes sense.