Math 525 Class 15 September 29

Problem 18, Section 9.1 p. 299.

Func(R) = ring of fcns $R \to R$.

here R is a ring (need not be commutative)

What is the multiplication on R?

Two candidates: multiplication in R.
composition of functions.

Do these work to create a ring structure on Func(R)?

if f, g, h functions $R \to R$.

we need. $f(g+h) = fg + fh$

and. $(f+g)h = fh + gh$.

if the multiplication in Func(R) is pointwise mult. Then need, $\forall a \in R$

$f(a)(g(a)+h(a)) = f(a)g(a) + f(a)h(a)$

and $(f(a)+g(a))h(a) = f(a)h(a) + g(a)h(a)$

This looks like it works.

Let's look at the other possibility.

$$f \circ (g+h) = fog + f \circ h$$

Doubtful, because f need not be a linear function: $Func(R)$ is ALL functions $R \to R$.

So $Func(R)$ defined by pointwise mult.

18 (b) Prove that $\varphi: R[x] \to Func(R)$ defined by $\varphi(p) = f_p$, that is

$$\varphi(p)(r) = p(r) \quad \text{for } r \in R.$$

is NOT a ring homomorphism in general.

Remark: in order to prove this we need to work with noncommutative rings.

We are given a hint connected to $R = \mathbb{H}$.

and the polyn. $p(x) = x^2 + 1 = (x+i)(x-i)$

Idea: check if the map φ preserves multiplication: we have

$$p(x) = x^2+1 = f(x)\,g(x)$$

where $f(x) = x+i$ $\quad g(x) = x-i$.

Is $\varphi(p) = \varphi(f)\,\varphi(g)$?

This requires $\varphi(p)(\alpha) = \varphi(f)(\alpha)\,\varphi(g)(\alpha)$ for all $\alpha \in \mathbb{H}$.

Let's check this for $\alpha = j$.

$$\varphi(p)(j) = j^2+1 = -1+1 = 0.$$

$$\varphi(f)(j)\cdot\varphi(g)(j) = (j+i)(j-i).$$

$$= j^2 - ji + ij - i^2$$

$$= -1 + ij + ij - (-1).$$

$$= 2ij \neq 0.$$

Q: Why, when multiplying $(x+i)(x-i)$ do we not write $x^2 - xi + ix - i^2$

and obtain $X^2+1+ix-xi \neq x^2+1$?

A: See "Defn of Polynomial Rings", p. 295.

Remarks on problem #11, Ch. 7 Sec 6.

"p-adic integers"

Philosophy: checking that ⟨fact⟩ is true in the p-adic integers is similar to checking that ⟨fact⟩ is true in $\mathbb{Z}/p^N\mathbb{Z}$ for arbitrarily large N.

So for part (e) of #11

(Recall that μ_{ji} defined in #11 to be projection: $\mu_{ji} : \mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$

$a \bmod p^j \mapsto a \bmod p^i$

(here $i \leq j$.)

To prove that element in inverse limit $\mathbb{Z}_p$ exists just prove that elements in $\mathbb{Z}/p^N\mathbb{Z}$

exist for all N.

Then If these elements are "consistent"

that is $\{x_i\} \in \mathbb{Z}/p^i\mathbb{Z}$ satisfies.

$$\mu_{ji}(x_j) = x_i$$

then $\lim_{i \to \infty} x_i$ exists in $\mathbb{Z}_p$.

So let's first try to solve this at the level of $\mathbb{Z}/p^j\mathbb{Z}$ for each j.

a_1 is an integer mod p, so take $a_1 \in \mathbb{Z}$.

So $a_1^{p-1} \equiv 1 \mod p$.

Let's find an a_2 such that

$a_2^{p-1} \equiv 1 \mod p^2$ and $\mu_{21}(a_2) = a_1$

Try $a_2 = a_1 + xp \mod p^2$

$$a_2^{p-1} = a_1^{p-1} + \binom{p-1}{1} a_1^{p-2} xp + \binom{p-1}{2} a_1^{p-3} x^2 p^2$$

$$\equiv a_1^{p-1} + (p-1)a_1^{p-2} x p \mod p^2$$

Plan: show that this equation can be solved for $x \in \mathbb{Z}/p\mathbb{Z}$.

and then continue inductively to obtain.

$a_3, a_4, \ldots$, etc.

How do we show that some such x exists?

We are asking that $a_2^{p-1} \equiv 1 \mod p^2$.

We know $a_1^{p-1} \equiv 1 \mod p$.

$a_1^{p-1} \equiv 1 + yp \mod p^2$. So equation for x:

$$a_2^{p-1} \equiv 1 \equiv 1 + yp + (p-1)a_1^{p-2} x p \mod p^2$$

We need $$0 \equiv yp + (p-1)a_1^{p-2} x p \mod p^2$$

$$0 \equiv y + (p-1)a_1^{p-2} x \mod p.$$

Solution $x \equiv (p-1)^{-1}(a_1^{p-2})^{-1}(-y) \bmod p.$

a_1 invertible mod p since $a_1^{p-1} \equiv 1 \bmod p.$

Suggestion: "Look up "Hensel's Lemma."

Read 9.4 for Monday and prepare for a quiz..

New Hw will be up today!