

Homework 19 - MATH 791

Will Thomas

Throughout this assignment R denotes a commutative ring.

Problem 1:

Let $I \subseteq R$ be an ideal, and $R[x]$ denote the polynomial ring in x over R . Let $I[x]$ denote the set of polynomials in R with coefficients in I and let $\langle I \rangle$ denote the ideal of $R[x]$ generated by the set I . Show that $I[x] = \langle I \rangle$.

Solution:

Let us start by defining the sets:

$$I[x] := \{i_n x^n + \cdots + i_0 \mid i_j \in I\}$$
$$\langle I \rangle := \{i_n x^n + \cdots + i_0 \mid i_j \in I\}$$

These sets are definitionally equal as is straightforward to see, with the ideal generated by I being equivalent due to the closure of the ideal.

Problem 2:

Maintaining the notation from 1, show that the rings $R[x]/I[x]$ and $(R/I)[x]$ are isomorphic.

Solution:

We can show this isomorphism by showing there is an onto ring homomorphism $\phi : R[x] \rightarrow (R/I)[x]$ and that $\ker(\phi) = I[x]$

Let us define $\phi(f(x)) = [f(x)]$ ($[f(x)]$ is the equivalence class).

First, we want to show the ring homomorphism property holds:

$$\forall f_1(x), f_2(x) \in R[x], \phi(f_1(x) + f_2(x)) = [f_1(x) + f_2(x)]$$

Due to it being an equivalence class, we can unfold this

$$[f_1(x) + f_2(x)] = [f_1(x)] + [f_2(x)] = \phi(f_1(x)) + \phi(f_2(x))$$

Addition holds, as for multiplication:

$$\forall f_1(x), f_2(x) \in R[x], \phi(f_1(x)f_2(x)) = [f_1(x)f_2(x)]$$

Due to it being an equivalence class, we can unfold this

$$[f_1(x)f_2(x)] = [f_1(x)][f_2(x)] = \phi(f_1(x))\phi(f_2(x))$$

Onto property:

$$\forall [f(x)] \in (R/I)[x], \exists f(x) \in R, \text{ s.t. } \phi(f(x)) = [f(x)]$$

Showing $\ker(\phi) = I[x]$:

$$\begin{aligned}\ker(\phi) &= \{f(x) \in R \mid \phi(f(x)) = [0]\} \\ &= \{[f(x)] = [0] \mid f(x) \in R\}\end{aligned}$$

This is $= I[x]$ as $[f(x)] = [0] \iff f(x) \in I[x]$

Using the first isomorphism theorem for rings, we can conclude then that

$$\therefore R[x]/I[x] \cong (R/I)[x]$$

Problem 3:

Let $R[[x]]$ denote the formal power series ring over R , i.e., the set of expressions of the form $\sum_{i=0}^{\infty} a_i x^i$, with $a_i \in R$. Note this is purely an algebraic expression and does not involve any notion of convergence. We add and multiply element of $R[[x]]$ in the expected way: If $f = \sum_{i=0}^{\infty} a_i x^i$ and $g = \sum_{i=0}^{\infty} b_i x^i$, then: $f + g = \sum_{i=0}^{\infty} (a_i + b_i) x^i$ and $fg = \sum_{k=0}^{\infty} c_k x^k$, where $c_k = \sum_{i+j=k} a_i b_j$. For $I \subseteq R$, let $I[[x]]$ denote the elements in $R[[x]]$, all of whose coefficients belong to I .

- (i) Verify that $R[[x]]$ is a ring and $I[[x]]$ is an ideal of $R[[x]]$.
- (ii) Show that if I is finitely generated, then $\langle I \rangle = I[[x]]$ as ideals of $R[[x]]$.
- (iii) Can you give an example where $I[[x]] \neq \langle I \rangle$

Solution:

- (i) To show that $R[[x]]$ is a ring, we need to show that it is an abelian group under addition, is closed under multiplication with an identity, and multiplication distributes over addition.

It is fairly straightforward to see that addition is an abelian group, additionally the multiplicative identity and closure are straightforward as well.

Show the distributive property:

$$\begin{aligned}\forall fgh, f(g+h) &= \sum_{l=0}^{\infty} d_l x^l, d_l = \sum_{i+j+k=l} a_i (b_j + c_k) \\ \implies d_l &= \sum_{i+j+k=l} (a_i b_j) + (a_i c_k) \implies f(g+h) = fg + gh\end{aligned}$$

Now, to show that $I[[x]]$ is the ideal of $R[[x]]$:

Since I is an ideal, then $I[[x]]$ will be an ideal as well, as the only multiplication and addition that will matter will affect the coefficients (which are in I). The closure is also inherent to the coefficients being in the ideal I .

(ii) In a very similar manner to problem 1, any element

$$i_j \in \langle I \rangle, \quad i_j * \sum_{i=0}^{\infty} a_i * x^i = \sum_{i=0}^{\infty} i_j * a_i * x^i \in I[[x]]$$

and vice versa and element in $I[[x]]$ can be factored out.

(iii) **Admitted**

Here is Eisenstein's Criterion, which is an important test for irreducibility of polynomials over a UFD.

Eisenstein's Criterion: Let R be a UFD with quotient field K . Suppose $f(x) = a_n x^n + \cdots + a_0 \in R[x]$ is a primitive polynomial. Let $p \in R$ be a prime element and suppose:

- (i) $p \mid a_i$, for all $0 \leq i < n$
- (ii) $p \nmid a_n$
- (iii) $p^2 \nmid a_0$.

Then $f(x)$ is irreducible over K (equivalently, over R).

For example, $x^6 + 10x^2 + 5x + 15$ is irreducible over \mathbb{Q} , by using Eisenstein's criterion and $p = 5$.

Problem 4:

Let $p \in \mathbb{Z}$ be prime and $f_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Z}[x]$. Use Eisenstein's criterion, together with the following fact to show that $f_p(x)$ is irreducible over $\mathbb{Q}[x]$: $f_p(x)$ is irreducible over \mathbb{Q} if and only if $f_p(x+1)$ is irreducible over \mathbb{Q} .

Solution:

First, let us analyze the fact that $f_p(x)$ irred. $\iff f_p(x+1)$ irred.

If $f_p(x)$ is irreducible, then $f_p(x+1) = (x+1)^{p-1} + \cdots + (x+1) + 1$, which we can reduce to

$$[x^{p-1} + \binom{p-1}{1}(x^{p-2})(1) + \cdots + \binom{p-1}{p-2}(x^1) + 1] + \cdots + [x + 1] + 1$$

From this we can subtract our $f_p(x)$ that is irreducible, and now that what is left must also be irreducible.

$$\therefore \sum_{i=0}^{p-1} \binom{p-1}{i} x^{p-1-i} \text{ is irreducible}$$

This conclusion lets us see that criterion (i) of Eisenstein's Criterion holds.

To show criterion (ii), it is fairly straightforward to see that any value of p will not divide $a_n = 1$ unless $p = 1 \implies f_p(x) = 1$ (which will be trivially irreducible)

Finally for criterion (iii), let us assume that $p^2 \mid a_0$. This would then mean that we could factor out p^2 from a_0 in both $f_p(x)$ and $f_p(x+1)$, which means in this case that $p^2 \mid 1 \implies p = 1 \rightarrow \leftarrow$

This would once again lead to the trivially irreducible $f_p(x) = 1$

\therefore We have proven all of Eisenstein's Criterion's, so $f_p(x)$ is irreducible

Problem 5:

Use Eisenstein's criterion and the fact that $\mathbb{Q}[x]$ is a UFD to show that $x^2 + y^2 - 9$ is irreducible in $\mathbb{Q}[x, y]$.

Solution:

we can use Eisenstein's criterion with prime element $p = 3$.

Clearly, $3 \mid -9$ and $3 \nmid 1$ so criterions (i), (ii) are fulfilled

To show that $3^2 \nmid -9$ we need to see that the unique factorization of -9 by irreducibles is $-9 = -1 * 3^2 * 1$

In order for -9 to be divisible by 3^2 we need an element $f(x, y)$ such that

$-9 = 3^2 * f(x, y)$ but this would violate the unique factorization of -9 by irreducibles as it would require that $3^2 \mid f(x, y)$ but $f(x, y) = -1$ and $3^2 \nmid -1$.

$$\therefore 3^2 \nmid -9$$

Thus $x^2 + y^2 - 9$ is irreducible in $\mathbb{Q}[x, y]$