HOMEWORK-1

SIDDHANT CHAUDHARY
BMC201953

4. Funny Ring Structure. Given a ring R, show that we get a new ring structure on the same *set* R as follows: define a new addition $\oplus$ by $a \oplus b = a + b - 1$ and a new multiplication $\odot$ by $a \odot b = a + b - ab$. You can prove this by going through the axioms, *but that is not the point of this exercise at all*. Instead prove the claim by simultaneously showing that the new ring structure is actually *isomorphic* to the original ring. (The basic observation is that if there is any *bijection* from a group/vector space/ring/whatever structure to some set S, then one can make S into the same structure by using f as a dictionary.)

Solution. As in the statement given in the parenthesis, it is enough to exhibit a bijection f from R to R which will act as a recipe for the funny ring structure. Consider the *set* map $f : R \to R$ given by

$$f(a) = 1 - a$$

It is clear that f is injective, because

$$1 - a = 1 - b \implies a = b$$

for any $a, b \in R$. Moreover, f is surjective, because given any $a \in R$ we have

$$f(1 - a) = 1 - (1 - a) = a$$

and so we conclude that f is a bijection. Now, we will use the bijection f as a recipe to give another ring structure to R. For any $a, b \in R$ we define operations $+_{\text{funny}}$ and $\cdot_{\text{funny}}$ as

$$a +_{\text{funny}} b := f(f^{-1}(a) + f^{-1}(b)) = a + b - 1 = a \oplus b$$
$$a \cdot_{\text{funny}} b := f(f^{-1}(a) \cdot f^{-1}(b)) = a + b - ab = a \odot b$$

and let

$$0_{\text{funny}} = f(0) = 1$$
$$1_{\text{funny}} = f(1) = 0$$

So, it follows that the operations $+_{\text{funny}}$ and $\oplus$ coincide, and $\cdot_{\text{funny}}$ and $\odot$ coincide. Moreover, R is a ring under the operations $+_{\text{funny}}$ and $\cdot_{\text{funny}}$ because the ring axioms hold for $+$ and $\cdot$, so they automatically hold for these new operations as well. Finally, by the above definition we have that

$$f(a + b) = f(a) \oplus f(b)$$
$$f(a \cdot b) = f(a) \odot f(b)$$

for *any* $a, b \in R$, implying that f is actually a *ring isomorphism* between R and the funny version of R (note that we didn't check $f(1) = 1_{\text{funny}}$, because that is

Date: November 2020.

a part of our definition). This shows that the funny ring is isomorphic to the original one, completing the proof.

Before doing problem **5.**, I will try to prove a general fact which was mentioned in Lecture 3. As a note, wherever I use the term *the gcd*, I mean the gcd upto units.

Proposition 0.1. *Let $p(x), g(x) \in \mathbb{Z}[x]$ be any two polynomials such that the gcd of the coefficients of $p(x)$ is 1, and the gcd of the coefficients of $g(x)$ is 1. Then, the gcd of the coefficients of $p(x)g(x)$ is also 1.*

Proof. For the sake of contradiction, suppose the gcd of the coefficients of $p(x)g(x)$ is not 1 (i.e not a unit). Also, suppose

$$p(x) = a_0 + a_1x + ... + a_nx^n$$
$$g(x) = b_0 + b_1x + ... + b_mx^m$$

Suppose the gcd of the coefficients of $p(x)g(x)$ is d, where d is not a unit (and clearly $d \neq 0$ as $p(x), g(x)$ are non-zero). So by prime factorisation in $\mathbb{Z}$, there is some prime factor P of d. So, P divides each coefficient of $p(x)g(x)$. But by our assumption, there are coefficients a_r and b_s such that P does not divide a_r and b_s. Pick the *largest* such r and s (i.e P divides a_i for each $i > r$, and P divides b_i for each $i > s$). We can choose the largest such r and s since we are dealing with polynomials, which have finitely many non-zero coefficients. Now the coefficient of the term x^{r+s} in $p(x)g(x)$ (which by assumption is divisible by P) is

$$\sum_{i=0}^{r+s} a_ib_{r+s-i} = a_rb_s + \sum_{i=0}^{r-1} a_ib_{r+s-i} + \sum_{i=r+1}^{r+s} a_ib_{r+s-i}$$

Now, if $0 \leq i \leq r-1$, then $r+s-i \geq s+1$, and hence $P|b_{r+s-i}$ for each such i. Similarly, if $i \geq r+1$, then $P|a_i$ for each such i. So, the above equation combined with these facts implies that $P|a_rb_s$. Since P is a prime, this implies that P divides one of a_r or b_s, but this is clearly a contradiction. Hence, this shows that the gcd of the coefficients of $p(x)g(x)$ must be a unit, i.e it must be 1. ■

Remark 0.1.1. I think the above proof can be modified to rings where factorization into irreducibles holds, but for now that is not important.

Corollary 0.1.1. *Let $p(x), g(x) \in \mathbb{Z}[x]$ be any two polynomials. Suppose d_1 is the gcd of the coefficients of $p(x)$ and d_2 is the gcd of the coefficients of $g(x)$. Then the gcd of the coefficients of $p(x)g(x)$ is d_1d_2.*

Proof. Clearly, we can write $p(x) = d_1p'(x)$ and $g(x) = d_2g'(x)$, where $p'(x), g'(x) \in \mathbb{Z}[x]$ such that the gcd of the coefficients of $p'(x)$ is 1, and the gcd of the coefficients of $g'(x)$ is also 1. Also, we see that

$$p(x)g(x) = d_1d_2p'(x)g'(x)$$

By **Proposition** 0.1, we know that the gcd of the coefficients of $p'(x)g'(x)$ is 1. Hence, it follows that the gcd of the coefficients of $p(x)g(x)$ is d_1d_2, completing the proof. ■

Proposition 0.2. *Let $\mathbb{Z}[x] \xrightarrow{\varphi} \mathbb{C}$ be a ring homomorphism such that $\varphi(x) = a$ for some $a \in \mathbb{C}$. Then,* Ker φ *is a principal ideal in $\mathbb{Z}[x]$.*

Proof. Throughout I will assume the standard inclusions $\mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{C}$ (and hence the standard inclusions of the corresponding polynomial rings as well). First, if Ker φ is trivial, then it is clear that Ker $\varphi = (0)$, i.e it is a principal ideal in $\mathbb{Z}[x]$. So, assume that the kernel is not trivial. So, there is some non-zero polynomial $d(x) \in \mathbb{Z}[x]$ such that $d(a) = 0$. Among all such polynomials, let $d(x)$ be the one with *least* degree such that the gcd of the coefficients of $d(x)$ is 1 (it is easy to see that choosing such a $d(x)$ is possible by factoring out the gcd if necessary). We claim that

$$\text{Ker } \varphi = (d(x))$$

To prove this, suppose $p(x) \in$ Ker φ. We know that $p(x)$ and $d(x)$ are both polynomials in the ring $\mathbb{Q}[x]$ (by the standard inclusion). Since $\mathbb{Q}$ is a field, **Euclidean Division** holds, and there are polynomials $q(x), r(x) \in \mathbb{Q}[x]$ such that

$$p(x) = q(x)d(x) + r(x)$$

where either $\deg r < \deg d$ or $r(x) = 0$. Let l_1 be the LCM of the denominators of the coefficients of $q(x)$, and similarly let l_2 be the LCM of the denominators of the coefficients of $r(x)$ (so that $l_1, l_2 \in \mathbb{Z} - \{0\}$). Then, we can write

$$q(x) = \frac{q'(x)}{l_1} \text{ and } r(x) = \frac{r'(x)}{l_2}$$

where $q'(x), r'(x) \in \mathbb{Z}[x]$. So we get

$$l_1 l_2 p(x) = l_2 q'(x)d(x) + l_1 r'(x)$$

and this is an equation in $\mathbb{Z}[x]$. Clearly, we see that

$$l_1 r'(a) = 0$$

and hence $r'(a) = 0$ as $l_1 \neq 0$. Since $\deg r'(x) = \deg r(x) < \deg d(x)$, by the *definition* of $d(x)$ it must be true that $r'(x) = 0$. Hence, we get

$$l_1 l_2 p(x) = l_2 q'(x)d(x) \implies l_1 p(x) = q'(x)d(x)$$

Suppose s is the gcd of the coefficients of $p(x)$. Then, the gcd of the coefficients of $l_1 p(x)$ is $l_1 s$, and hence the gcd of the coefficients of $q'(x)d(x)$ is $l_1 s$. By our assumption, the gcd of the coefficients of $d(x)$ was 1, and hence it must be true that the gcd of the coefficients of $q'(x)$ is $l_1 s$ (this is where we apply **Corollary** 0.1.1). All this fuss was to show that

$$\frac{q'(x)}{l_1} \in \mathbb{Z}[x]$$

so that $p(x)$ is a $\mathbb{Z}[x]$-multiple of $d(x)$. This shows that

$$\text{Ker } \varphi \subseteq (d(x))$$

Conversely, any $\mathbb{Z}[x]$-multiple of $d(x)$ is clearly a member of Ker φ. This completes the proof. ■

5. Artin Chapter 11: 3.3 c and e on kernel of maps from polynomial rings. Find as few (and as simple) generators as you can.

Solution. For **3.3 c**, the map is $\mathbb{Z}[x] \xrightarrow{\varphi} \mathbb{R}$ given by $f(x) \mapsto f(1+\sqrt{2})$, which is equivalent to saying $\varphi(x) = 1 + \sqrt{2}$. Via the standard inclusion $\mathbb{R} \hookrightarrow \mathbb{C}$, we can interpret this as a homomorphism $\mathbb{Z}[x] \xrightarrow{\varphi} \mathbb{C}$. Now we can just apply **Proposition 0.2**. Observe that if $d(x) = (x-1)^2 - 2$, then

$$d(1+\sqrt{2}) = 0$$

and hence Ker φ is non-trivial. Now, no *linear polynomial* in $\mathbb{Z}[x]$ has $1+\sqrt{2}$ as one of its roots, because $1+\sqrt{2}$ is an irrational number. So, $d(x)$ is infact a non-zero polynomial of least degree in Ker φ. Moreover, it is easily seen that the gcd of the coefficients of $d(x)$ is 1, and hence by **Proposition 0.2**, we see that

$$\text{Ker } \varphi = (d(x)) = ((x-1)^2 - 2)$$

For **3.3 e**, the map is $\mathbb{C}[x,y,z] \xrightarrow{\varphi} \mathbb{C}[t]$ that is identity on $\mathbb{C}$ and maps $x \mapsto t$, $y \mapsto t^2$ and $z \mapsto t^3$. Observe that the polynomials $f_1(x,y,z) = y - x^2$ and $f_2(x,y,z) = z - x^3$ are in the kernel of this homomorphism. I claim that

$$\text{Ker } \varphi = (f_1, f_2) = (y - x^2, z - x^3)$$

First, suppose $g(x,y,z) \in (y-x^2, z-x^3)$, so that

$$g(x,y,z) = r_1(x,y,z)(y-x^2) + r_2(x,y,z)(z-x^3)$$

for some $r_1, r_2 \in \mathbb{C}[x,y,z]$. In this case, it is clear that $g(x,y,z) \in$ Ker φ, and hence $(y-x^2, z-x^3) \subseteq$ Ker φ. We now show the reverse inclusion. Suppose $g(x,y,z) \in$ Ker φ, which means that

$$g(t, t^2, t^3) = 0$$

We know that $\mathbb{C}[x,y,z] \cong \mathbb{C}[x,y][z]$. Moreover, $z - x^3$ is a monic polynomial in $\mathbb{C}[x,y][z]$. So, applying **Euclidean Division** in $\mathbb{C}[x,y][z]$, we see that

$$g(x,y,z) = q(x,y,z)(z-x^3) + r(x,y,z)$$

for some $q, r \in \mathbb{C}[x,y,z]$ such that either $r = 0$, or the degree of z in R is less than 1, i.e $r(x,y,z)$ does not contain any monomial involving z, so that $r(x,y,z) \in \mathbb{C}[x,y]$. So for ease of notation, let us write $r(x,y,z) = r(x,y)$, and hence

$$g(x,y,z) = q(x,y,z)(z-x^3) + r(x,y)$$

Now, since $g(x,y,z)$ and $z - x^3$ are in Ker φ, it follows that $r(x,y) \in$ Ker φ, i.e

$$r(t, t^2) = 0$$

Now, we will apply a very similar reasoning again. We know that $\mathbb{C}[x,y] \cong \mathbb{C}[x][y]$, and $y - x^2$ is a monic polynomial in $\mathbb{C}[x][y]$. So by **Euclidean Division** in $\mathbb{C}[x][y]$, we have

$$r(x,y) = q'(x,y)(y-x^2) + r'(x,y)$$

for some $q', r' \in \mathbb{C}[x,y]$ such that either $r'(x,y) = 0$, or the degree of y in $r'(x,y)$ is less than 1, i.e $r'(x,y)$ does not contain any monomial involving y. So again, for easy of notation, we write $r'(x,y) = r'(x)$. Again, because $r(x,y), y - x^2 \in$ Ker φ, it follows that $r'(x) \in$ Ker φ, which implies that

$$r'(t) = 0$$

But because $r'(x)$ is a polynomial in x, it must be true that $r'(x) = 0$. So, we have

$$r(x,y) = q'(x,y)(y-x^2)$$

Putting it all together, we obtain

$$g(x,y,z) = q(x,y,z)(z-x^3) + q'(x,y)(y-x^2)$$

which shows that $g \in (y-x^2, z-x^3)$, and hence showing Ker $\varphi \subseteq (y-x^2, z-x^3)$. So this shows that

$$\text{Ker } \varphi = (y-x^2, z-x^3)$$

Remark 0.2.1. Above, I used the fact that $\mathbb{C}[x,y,z] \cong \mathbb{C}[x,y][z] \cong \mathbb{C}[x][y][z]$. These kind of isomorphisms of polynomials rings are not difficult to prove, but I couldn't include a proof because the document is already too long.

6. Artin Chapter 11: 3.6 and 3.7 on ring automorphisms of $R[x,y]$ and of $\mathbb{Z}[x]$. Do these exercises cleanly by using substitution principle as much as you can. While it is true that an isomorphism is a bijective ring homomorphism, it may be better to think of it equivalently as a (ring) map f such that there is an inverse (ring) map g in the opposite direction, i.e such that $f \circ g$ and $g \circ f$ are the respective identity maps.

Solution. First, we do **3.6**. Let R be any ring, and let $f(y)$ be a fixed polynomial in $R[y]$. We show that the map $R[x,y] \to R[x,y]$ defined by $x \mapsto x + f(y)$ and $y \mapsto y$ is an *automorphism* of $R[x,y]$, and we will use the substitution principle to do this. Let $R \xrightarrow{\iota} R[x,y]$ be the standard inclusion map (which is clearly a homomorphism). By the substitution principle, there is a *unique* homomorphism $R[x,y] \xrightarrow{\varphi} R[x,y]$ such that $\varphi(x) = x + f(y), \varphi(y) = y$ and the following diagram commutes.

$$\begin{tikzcd} R \arrow[r, "\iota"] \arrow[d, "\iota"] & R[x,y] \arrow[dl, "\varphi"] \\ R[x,y] & \end{tikzcd}$$

Again, by the substitution principle, there is a *unique* homomorphism $R[x,y] \xrightarrow{\Phi} R[x,y]$ such that $\Phi(x) = x - f(y), \Phi(y) = y$ and the following diagram commutes.

$$\begin{tikzcd} R \arrow[r, "\iota"] \arrow[d, "\iota"] & R[x,y] \arrow[dl, "\Phi"] \\ R[x,y] & \end{tikzcd}$$

We will now show that $R[x,y] \xrightarrow{\Phi\circ\varphi} R[x,y]$ is the *identity* homomorphism, and a similar proof will show that $R[x,y] \xrightarrow{\varphi\circ\Phi} R[x,y]$ is the identity homomorphism, and that will show that φ is an *automorphism*, which will complete our proof. So, let $p \in R[x,y]$ be any element given by the multi-index notation

$$p(x,y) = \sum_{(i_1,i_2)\in\mathbb{Z}^2_{\geq 0}} a_{(i_1,i_2)} x^{i_1} y^{i_2}$$

(where the above sum is finite). We have

$$\begin{aligned}
\varphi(p) &= \varphi\left(\sum_{(i_1,i_2)\in\mathbb{Z}^2_{\geq 0}} a_{(i_1,i_2)}x^{i_1}y^{i_2}\right) \\
&= \sum_{(i_1,i_2)\in\mathbb{Z}^2_{\geq 0}} \varphi(a_{(i_1,i_2)}x^{i_1}y^{i_2}) \\
&= \sum_{(i_1,i_2)\in\mathbb{Z}^2_{\geq 0}} \varphi(a_{(i_1,i_2)})[\varphi(x)]^{i_1}[\varphi(y)]^{i_2} \\
&= \sum_{(i_1,i_2)\in\mathbb{Z}^2_{\geq 0}} a_{(i_1,i_2)}[x+f(y)]^{i_1}y^{i_2}
\end{aligned}$$

where in the last step we used the fact that φ restricts to the inclusion on R. So, we have that

$$\begin{aligned}
\Phi(\varphi(p)) &= \Phi\left(\sum_{(i_1,i_2)\in\mathbb{Z}^2_{\geq 0}} a_{(i_1,i_2)}[x+f(y)]^{i_1}y^{i_2}\right) \\
&= \sum_{(i_1,i_2)\in\mathbb{Z}^2_{\geq 0}} \Phi(a_{(i_1,i_2)}[x+f(y)]^{i_1}y^{i_2}) \\
&= \sum_{(i_1,i_2)\in\mathbb{Z}^2_{\geq 0}} \Phi(a_{(i_1,i_2)})[\Phi(x+f(y))]^{i_1}[\Phi(y)]^{i_2} \\
&= \sum_{(i_1,i_2)\in\mathbb{Z}^2_{\geq 0}} a_{(i_1,i_2)}x^{i_1}y^{i_2} \\
&= p(x,y)
\end{aligned}$$

where in the second last step, we used the fact that Φ restricts to the inclusion on R and that

$$\Phi(x+f(y)) = \Phi(x) + \Phi(f(y)) = x - f(y) + f(y) = x$$

So, this shows that $\Phi\circ\varphi = \text{id}_{R[x,y]}$, and hence by the discussion above this shows that φ is an automorphism.

Next, we find all automorphisms of the polynomial ring $\mathbb{Z}[x]$. Suppose $\mathbb{Z}[x] \xrightarrow{\varphi} \mathbb{Z}[x]$ is an automorphism. Consider the restriction $\varphi|_{\mathbb{Z}}$, which is a homomorphism from $\mathbb{Z}$ to $\mathbb{Z}[x]$. We know that there is only one homomorphism from $\mathbb{Z}$ to any ring, i.e the characteristic homomorphism. In this case, $\varphi|_{\mathbb{Z}}$ is simply the standard inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}[x]$. Now suppose $x \xrightarrow{\varphi} f(x)$, where $f(x) \in \mathbb{Z}[x]$ is some polynomial of degree n, where $n \geq 1$ ($n = 0$ is not possible since φ is surjective). So, for any polynomial $p(x) \in \mathbb{Z}[x]$ of degree $m \geq 1$, we see that

$$p(x) \xrightarrow{\varphi} p(f(x)) \quad \text{(this uses the fact that } \varphi|_{\mathbb{Z}}\text{) is the inclusion}$$

and since $\mathbb{Z}$ is an integral domain, we see that $p(f(x))$ has degree mn. From this, it follows that $n = 1$ is the only valid possibility, because otherwise the image of φ will *not* contain any polynomial of degree 1. So, suppose $x \xrightarrow{\varphi} ax + b$ for some $a, b \in \mathbb{Z}$, $a \neq 0$. We know that the polynomial x is in the range of φ. By the above discussion, its pre-image must be a linear polynomial, i.e suppose

$$cx + d \xrightarrow{\varphi} x$$

for some $c, d \in \mathbb{Z}$ with $c \neq 0$. But, we know that

$$\begin{aligned}\varphi(cx+d) &= \varphi(cx) + \varphi(d)\\ &= \varphi(c)\varphi(x) + \varphi(d)\\ &= c(ax+b) + d\\ &= cax + cb + d\end{aligned}$$

where we have again used the fact that $\varphi|_{\mathbb{Z}}$ is the inclusion map. So, we see that $cax + cb + d = x$, and this means that c, a are units in $\mathbb{Z}$, and hence $a = \pm 1$. So, it follows that $x \xrightarrow{\varphi} \pm x + b$, where $b \in \mathbb{Z}$.

Conversely, let us show that the unique homomorphism $\mathbb{Z}[x] \xrightarrow{\varphi} \mathbb{Z}[x]$ given by

$$x \xrightarrow{\varphi} x + b$$

for some $b \in \mathbb{Z}$ is an automorphism of $\mathbb{Z}[x]$ (and a similar proof will work for $x \xrightarrow{\varphi} -x + b$). To do this, we just need to exhibit an inverse for φ. Consider the unique homomorphism $\mathbb{Z}[x] \xrightarrow{\Phi} \mathbb{Z}[x]$ given by

$$x \xrightarrow{\Phi} x - b$$

Let us show that $\Phi \circ \varphi$ is the identity mapping, and a similar proof will show that $\varphi \circ \Phi$ is the identity mapping, and that will show that φ is an automorphism. But this is easy to see, because for any $p(x) \in \mathbb{Z}[x]$, we have

$$\Phi(\varphi(p(x))) = \Phi(p(x+b)) = p(x - b + b) = p(x)$$

and this shows that $\Phi \circ \varphi = \mathrm{id}_{\mathbb{Z}[x]}$. So, φ is an automorphism of $\mathbb{Z}[x]$. Hence, all automorphisms φ of $\mathbb{Z}[x]$ restrict to the inclusion map on $\mathbb{Z}$ and are of the form $x \xrightarrow{\varphi} \pm x + b$ for some $b \in \mathbb{Z}$.

Proposition 0.3 (**Frobenius Map**). *Let R be a ring of prime characteristic p. Then the map $R \to R$ defined by $x \mapsto x^p$ is a ring homomorphism.*

Proof. We will prove this using the binomial theorem for commutative rings (which was proven in Lecture 1). Suppose $x, y \in R$. Then, we know that

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}$$

where for any $c \in \mathbb{Z}_{\geq 0}$,

$$cx := x + x + x + ... + x \quad (c \text{ times})$$

Now suppose $1 \leq k < p$. We have

$$\binom{p}{k} = \frac{p(p-1)!}{k!(p-k)!}$$

Because p is a prime, for such a k we see that

$$\frac{(p-1)!}{k!(p-k)!}$$

is an integer. So, we have shown that $p|\binom{p}{k}$ for each $1 \leq k < p$. Consequently, because R has characteristic p, we see that for $1 \leq k < p$

$$\binom{p}{k} x^k y^{n-k} = 0$$

So, we have

$$(x+y)^p = x^p + y^p$$

so that the map $x \mapsto x^p$ preserves addition. Moreover, for any $x, y \in R$ we have

$$(xy)^p = x^p y^p$$

and hence the map preserves multiplication as well. Finally,

$$1^p = 1$$

and so this shows that the map is a ring homomorphism, completing the proof. ■

7. Artin Chapter 11: 3.9 on nilpotent/unipotent elements. You may appeal to the very standard Frobenius map in exercise 3.8, but prove it for yourself! (The definition used here is non-standard. Usual ring theory definition is unipotent = 1 + nilpotent, but here use the given definition.)

Solution. **(a)** Suppose $x \in R$ is a nilpotent element, i.e

$$x^n = 0$$

for some $n > 0$. Let us show that $(1+x)$ is a unit in R. Consider the usual algebraic identity

$$x^k - 1 = (x-1)(1 + x + ... + x^{k-1})$$

(the proof is by expanding the RHS) for any $x \in R$ and $k > 0$. Here 1 is the multiplicative identity of the ring R. Replacing x by $-x$ in the above equation, we see that

$$(-x)^k - 1 = (-x-1)(1 - x + x^2 - ... + (-1)^{k-1}x^{k-1})$$

and multiplying by -1 on both sides, we get

$$-(-x)^k + 1 = (x+1)(1 - x + x^2 - ... + (-1)^{k-1}x^{k-1})$$

Now, put $k = n$ above. Since $x^n = 0$, we see that $-(-x)^n = -(-1)^n x^n = 0$, and hence

$$1 = (x+1)(1 - x + x^2 - ... + (-1)^{n-1}x^{n-1})$$

which shows that $(1+x)$ is a unit in R.
(b) Suppose R has prime characteristic $p \neq 0$. Suppose a is a nilpotent element, then we show that $(1+a)$ is *unipotent*, i.e some power of $(1+a)$ is 1. Suppose $n > 0$ is such that $a^n = 0$. We know that the map $R \xrightarrow{\varphi} R$ given by $x \xrightarrow{\varphi} x^p$ (the **Frobenius Map** 0.3) is a ring homomorphism. Let k be a positive integer such that $p^k > n$. Then, applying the Frobenius map to $(1+a)$ k times, we see that

$$(1+a)^{p^k} = \varphi^k(1+a) = \varphi^{k-1}(1^p + a^p) = \varphi^{k-2}(1^{p^2} + a^{p^2}) = ... = \varphi(1^{p^{k-1}} + a^{p^{k-1}}) = 1^{p^k} + a^{p^k} = 1$$

and hence this shows that $(1+a)$ is a unipotent element, completing the proof.

8. Artin Chapter 11: 2.2 on units in $F[[t]]$ + 3.10 on ideals in $F[[t]]$. Which of the ideals you found are maximal? Which are prime?

Solution. To make things easier, I will denote the formal power series $(a_0, a_1, a_2, ...)$ as

$$a_0 + a_1 t + a_2 t^2 + ... = \sum_{n=0}^{\infty} a_n t^n$$

We claim that the only units in the ring $F[[t]]$ are those power series which have a non-zero constant term. To prove this, suppose

$$\sum_{n=0}^{\infty} a_n t^n \cdot \sum_{n=0}^{\infty} b_n t^n = 1$$

i.e $(a_0, a_1, ...)$ and $(b_0, b_1, ...)$ are units in $F[[t]]$. This implies that $a_0 b_0 = 1$, i.e $a_0, b_0 \neq 0$. Conversely, suppose $(a_0, a_1, a_2, ...)$ is an element of $F[[t]]$ such that $a_0 \neq 0$. Then, define

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

and inductively define

$$b_n := -a_0^{-1} \sum_{k=1}^{n} a_k b_{n-k}$$

for $n \geq 1$. In that case, it is easily seen that $a_0 b_0 = 1$ and for any $n \geq 1$,

$$\sum_{k=0}^{n} a_k b_{n-k} = 0$$

implying that

$$\sum_{n=0}^{\infty} a_n t^n \cdot \sum_{n=0}^{\infty} b_n t^n = 1$$

and hence $(a_0, a_1, a_2, ...)$ is a unit in $F[[t]]$. This completes the proof and characterises all units of $F[[t]]$.

Next, we compute all ideals of $F[[t]]$. I claim that all the ideals of $F[[t]]$ are the trivial ideals 0 and $F[[t]]$, and (t^n) for $n \geq 1$. It is clear that for any $n \geq 1$, (t^n) is an ideal of $F[[t]]$. Conversely, let I be any non-trivial ideal of $F[[t]]$. Since I is non-trivial, it is non-empty. Now, among all elements of I, let $(a_0, a_1, a_2, ...) \in I$ be a non-zero element such that the number

$$n := \text{min}\{i \geq 0 \mid a_i \neq 0\}$$

is minimal. Observe that $n = 0$ is not possible, because otherwise the element $(a_0, a_1, a_2, ...)$ will be a *unit* in $F[[t]]$, which will imply that $I = F[[t]]$, and that contradicts our assumption that I is a proper ideal. So, $n \geq 1$. We will show that $I = (t^n)$. Observe that by our notation

$$(a_0, a_1, a_2, ...) = (a_n t^n + a_{n+1} t^{n+1} + ...) = t^n \cdot (a_n + a_{n+1} t + ...) = t^n \cdot (a_n, a_{n+1}, a_{n+2}, ...)$$

Now, because $a_n \neq 0$, we see that the element $(a_n, a_{n+1}, a_{n+2}, ...)$ is a unit in $F[[t]]$, and hence it follows that $t^n \in I$, implying that $(t^n) \subseteq I$. To prove the reverse inclusion, suppose $(b_0, b_1, b_2, ...) \in I$, and we see that the number

$$r := \text{min}\{i \geq 0 \mid b_i \neq 0\}$$

satisfies $r \geq n$. So, we see that

$$(b_0, b_1, b_2, ...) = (b_r t^r + b_{r+1} t^{r+1} + ...) = t^n \cdot (b_r t^{r-n} + b_{r+1} t^{r+1-n} + ...) \in (t^n)$$

and this implies that $I \subseteq (t^n)$, and hence it follows that $I = (t^n)$. So, we have characterised all the ideals of $F[[t]]$.

Finally, we determine which of these ideals are maximal and which are prime. It is very clear that (t) is the only maximal ideal $F[[t]]$, since the only ideals containing (t) are itself and $F[[t]]$. For any $n > 1$, the ideal (t^n) is contained in (t), and hence it is not maximal. Now, since (t) is a maximal ideal, it is a prime ideal as well. Now, we will see that the only prime ideals of $F[[t]]$ are 0 and (t). To show this, suppose $n > 1$. Now, observe that

$$t^n = t^{n-1} \cdot t$$

which implies that t^n divides $t^{n-1} \cdot t$. However, it is easy to see that t^n cannot divide either of t^{n-1} or t, and hence it follows that (t^n) is not a prime ideal. So, it follows that the *only* maximal ideal is (t), and the *only* prime ideals are 0 and (t).

Notation. Let D be any ring, and let $f(x) \in D[x]$ be any non-zero polynomial. Let $c \in D$ be a root of $f(x)$. I will use the notation $m_{f(x)}(c)$ to denote the *multiplicity* of c as a root of $f(x)$, where *multiplicity* is as defined in problem **9.**

Lemma 0.4. *Let D be an integral domain, and let $c_0 \in D$ be fixed. Suppose*

$$f(x) = (x - c_0)^m q(x)$$

for some non-zero polynomial $q(x) \in D[x]$ and $m \geq 0$. Suppose $c \neq c_0$ is a root of $f(x)$. Then, c is a root of $q(x)$, and

$$m_{q(x)}(c) = m_{f(x)}(c)$$

Proof. First, because D is an integral domain and $c \neq c_0$, it follows that c must be a root of $q(x)$, and hence this means that $m_{q(x)}(c) \geq 1$. Also, since $q(x)$ is a factor of $f(x)$, the *definition* of multiplicity implies

$$m_{q(x)}(c) \leq m_{f(x)}(c)$$

Now, we prove the reverse inequality. We know that $(x - c)^{m_{f(x)}(c)}$ is a factor of $f(x)$, and hence it is a factor of $(x - c_0)^m q(x)$. Since D is an integral domain and $c \neq c_0$, we see that c is a root of $q(x)$, so that $q(x) = (x - c)q'(x)$ for some non-zero $q'(x) \in D[x]$. So, we see that

$$(x - c)^{m_{f(x)}(c)} | (x - c_0)^m (x - c) q'(x)$$

and the cancellation law in the integral domain $D[x]$ implies that

$$(x - c)^{m_{f(x)}(c) - 1} | (x - c_0)^m q'(x)$$

Repeating the same argument $m_{f(x)}(c) - 1$ times, it will imply that

$$(x - c)^{m_{f(x)}(c)} | q(x)$$

which implies that

$$m_{f(x)}(c) \leq m_{q(x)}(c)$$

and hence we conclude that

$$m_{q(x)}(c) = m_{f(x)}(c)$$

and this completes the proof. ∎

9. For c in a ring D and non-zero $f(x)$ in $D[x]$, define the *multiplicity* of c as a root of $f(x)$ to be the largest non-negative integer n such that $f(x) = (x-c)^n q(x)$ in $D[x]$. Observe that this is well defined.
(i) In a *domain* D, show that

$$\prod_{c \text{ root of } f(x)} (x-c)^{\text{multiplicity of } c \text{ as a root of } f(x)}$$

is a factor of $f(x)$. This generalizes an exercise done in the lecture.
(ii) Find a counterexample to **(i)** where D is not a domain and f is a *monic* polynomial with a root whose multiplicity equals your roll number.
(iii) For a finite field F of cardinality q, show that

$$x^q - x = \prod_{c \in F} (x-c)$$

You do NOT need to use the fact that $F[x]$ has the unique factorization property. (Hint: the set of nonzero elements in F form a group under multiplication. The order of each element of a finite group is a factor of the order of the group.)

Solution. (i) Suppose D is an integral domain. Suppose $f(x) \in D[x]$ is a non-zero polynomial. For a root c of $f(x)$, we will use the notation $m_{f(x)}(c)$ to denote the *multiplicity* of c as a root of $f(x)$. We will show that

$$\prod_{c \text{ root of } f(x)} (x-c)^{m_{f(x)}(c)}$$

is a factor of $f(x)$. Observe that the above product is finite, since non-zero polynomials in integral domains have finitely many roots. We will prove the claim by induction on the degree of $f(x)$. For the base case, we have deg $f(x) = 0$, i.e $f(x)$ is a constant (non-zero) polynomial. In that case, the claim is trivially true, because the product will be empty. So the base case is true. Now suppose the statement is true for all non-zero polynomials of degree atmost n, and let $f(x) \in D[x]$ be a non-zero polynomial of degree $n+1$. If $f(x)$ has no roots in D, then the product

$$\prod_{c \text{ root of } f(x)} (x-c)^{m_{f(x)}(c)}$$

is empty, and in that case the statement still holds. So, suppose $f(x)$ has a root c_0 in D. By the **Factor Theorem**, it follows that $(x-c_0)$ is a factor of $f(x)$, and this means that $m_{f(x)}(c_0) \geq 1$. By the *definition* of multiplicity, we see that

$$f(x) = (x-c_0)^{m_{f(x)}(c_0)} q(x) \tag{†}$$

for some non-zero polynomial $q(x) \in D[x]$, and clearly deg$(q(x)) <$ deg$(f(x))$. Now, if c_0 is the *only* root of $f(x)$, then

$$\prod_{c \text{ root of } f(x)} (x-c)^{m_{f(x)}(c)} = (x-c_0)^{m_{f(x)}(c_0)}$$

and this is clearly a factor of $f(x)$. Now suppose c is any *other* root of $f(x)$, i.e $c \neq c_0$. **Lemma** 0.4 then implies that c is a root of $q(x)$ and

$$m_{q(x)}(c) = m_{f(x)}(c)$$

Now, applying the induction hypothesis on $q(x)$, we see that

$$\prod_{c \neq c_0 \text{ root of } f(x)} (x-c)^{m_{f(x)}(c)}$$

is a factor of $q(x)$. Then, equation (†) implies that

$$\prod_{c \text{ root of } f(x)} (x-c)^{m_{f(x)}(c)}$$

is a factor of $f(x)$. So by induction, the statement follows for all non-zero polynomials in $D[x]$, completing the proof.

(ii) Let $D = \mathbb{Z}/4\mathbb{Z}$, and evidently D is not an integral domain. Consider the polynomial

$$f(x) = x^{201953}$$

(my roll number is BMC201953). Clearly, the root $x = 0$ has multiplicity 201953 for this polynomial. Moreover, observe that

$$f(2) = 2^{201953} = 2^2 \cdot 2^{201951} = 0$$

and hence this means that 2 is also a root of $f(x)$, implying that $x-2$ is a factor of $f(x)$ by the **Factor Theorem**. This means that $m_{f(x)}(2) \geq 1$. Moreover, since 1 and 3 are units modulo 4, it follows that the only roots of f are 0 and 2. Now, note that

$$\prod_{c \text{ root of } f(x)} (x-c)^{m_{f(x)}(c)} = x^{201953}(x-2)^{m_{f(x)}(2)}$$

and hence the above polynomial has degree greater than 201953, since $m_{f(x)}(2) \geq 1$. This means that the above polynomial *cannot* be a factor of $f(x)$, since in any ring a polynomial cannot have a monic factor of degree greater than itself. Since $f(x)$ is itself monic, this gives us the required counterexample.

(iii) Let F be a finite field of cardinality q. We show that

$$x^q - x = \prod_{c \in F} (x-c)$$

First, we show that if $y \in F$, then $y^q - y = 0$. This is clear if $y = 0$, so suppose $y \neq 0$. So, y must be a unit in F. Now we know that the set of units of F form a group under multiplication, and this group has $q-1$ elements since F has $q-1$ units. So, the order of y must be a factor of $q-1$ (the order of the group), and hence we see that

$$y^{q-1} = 1$$

which implies that

$$y^q - y = 0$$

Now, this means that every $y \in F$ is a root of the polynomial $x^q - x$. So by **Factor Theorem**, it follows that $x-c$ divides $x^q - x$ for every $c \in F$. Using the fact that F is an integral domain and applying the **Factor Theorem** q times, we see that

$$x^q - x = g(x) \prod_{c \in F} (x-c)$$

for some polynomial $g(x) \in F[x]$. Clearly, $g(x) \neq 0$. Also, the degree of the polynomial

$$\prod_{c \in F} (x-c)$$

is q, and hence it follows that the degree of $g(x)$ must be 0, i.e $g(x) = y$ for some unit $y \in F$. Moreover, since $x^q - x$ and $\prod_{c \in F} (x - c)$ are monic, it follows that $y = 1$. So, it follows that

$$x^q - x = \prod_{c \in F} (x - c)$$

and this completes the proof.