Exercise 1 Let k be a field and $f(x) \in k[x] \setminus \{0\}$. TFAE:

- (a) The ideal (f(x)) is prime
- (b) (f(x)) is maximal
- (c) f(x) is irreducible

Proof. • $((a) \Rightarrow (c))$

Let (f(x)) be prime, therefore k[x]/(f(x)) is an integral domain. So assume that:

$$f(x) = g(x)h(x)$$
, for some $g, h \in k[x]$ (1)

$$\Rightarrow 0 = (g(x) + (f(x)))(h(x) + (f(x))) \tag{2}$$

Since k[x]/(f(x)) is entire, this implies that on of these factors is zero. WLOG assume that:

$$g(x) + (f(x)) = 0 \Rightarrow g(x) \in (f(x))$$
(3)

 $\therefore g(x) = c(x)f(x)$, for some $c(x) \in k[x]$. But since:

$$f(x) = g(x)h(x) = c(x)h(x)f(x) \Rightarrow f(x)(1 - c(x)h(x)) = 0$$
(4)

So by the fact that k[x] is a PID c(x)h(x) = 1, so we have $c(x), h(x) \in k[x]^* = k$. Since this is true for any arbitrary factors, we indeed see that f is irreducible.

• $((c) \Rightarrow (b))$

Let f(x) be irreducible and let $g(x) \notin (f(x))$. Since k[x] is a PID, there exists $h \in k[x]$ such that:

$$(f(x), g(x)) = (h(x)) \tag{5}$$

$$\therefore \begin{cases} f(x) = h(x)q(x) \text{ for some } q \in k[x] \\ g(x) = h(x)p(x) \text{ for some } p \in k[x] \end{cases}$$

Since we have that f is irreducible we have two cases: $h(x) \in k = k[x]^*$, or h(x) = af(x) for some $a \in k$.

But notice that the second case is impossible since it would imply that $g(x) = af(x)p(x) \in (f(x))$.

So we then see that (h(x)) = (1) = k[x].

But this argument tells us that any ideal, \mathcal{I} , that properly contains (f(x)) will contain an element $g(x) \notin (f(x))$, so

$$k[x] = (f(x), g(x)) \subseteq \mathcal{I} \subseteq k[x] \Rightarrow \mathcal{I} = k[x] \tag{6}$$

So (f(x)) is indeed maximal.

• $((b) \Rightarrow (a))$

Recall, by theorem it was already shown in this textbook that all maximal ideals are prime.

Remark. I don't really understand why this question is in the polynomial section, since this fact is true for any PID.

Exercise 2

Exercise 3 Let $f \in k[x]$, and x, y be two variables; show that in k[x] we have a "Taylor series" expression

$$f(x+y) = f(x) + \sum_{i=1}^{n} \varphi_i(x) y^i$$
, where $\varphi_i \in k[x] \ \forall i$

Furthermore, if k has character 0 then:

$$\varphi_i = \frac{D^i f(x)}{i!}$$

Proof. Let $a_i \in k$ be such that, $f(x) = \sum_{i=0}^n a_i x^i$, then we have

$$f(x+y) = \sum_{i=0}^{n} a_i (x+y)^i$$
 (1)

$$= \sum_{i=0}^{n} a_i \sum_{k=0}^{i} {i \choose k} x^{i-k} y^k \tag{2}$$

$$= \sum_{i=0}^{n} (a_i x^i + a_i \sum_{k=1}^{i} {i \choose k} x^{i-k} y^k)$$
 (3)

$$= \sum_{i \neq 0}^{n} a_i x^i + \sum_{i=1}^{n} \sum_{k=1}^{i} a_i \binom{i}{k} x^{i-k} y^k$$
(4)

(5)

Now note that by re-arraging terms we have:

$$\sum_{i=1}^{n} \sum_{k=1}^{i} \binom{i}{k} x^{i-k} y^k = \sum_{k=1}^{n} \left(\sum_{i=k}^{n} a_i \binom{i}{k} x^{i-k} \right) y^k \tag{6}$$

So if we let $\varphi_i(x) = \sum_{k=i}^n a_k \binom{k}{i} x^{k-i}$, we see that:

$$f(x+y) = f(x) + \sum_{i=1}^{n} \varphi_i(x)y^i$$
(7)

Now assume that k has character 0, we will inductively find a formula for $D^i f(x)$:

•

$$D^{1}f(x) = D(\sum_{k=0}^{n} a_{k}x^{k}) = \sum_{k=1}^{n} (a_{k} \cdot k)x^{k-1}$$
(8)

• If $D^i f(x) = \sum_{k=i}^n (a_k \cdot k(k-1) \cdots (k-i-1)) x^{k-i}$, we have that

$$D^{i+1}f(x) = D(D^{i}f(x)) = D(\sum_{k=i}^{n} (a_k \cdot k(k-1) \cdot \dots \cdot (k-i-1))x^{k-i}) = \sum_{k=i+1}^{n} (a_k \cdot k(k-1) \cdot \dots \cdot (k-i-1)(k-i))x^{k-(i+1)}$$
(9)

Therefore we see that for all i we have $D^i f(x) = \sum_{k=i}^n (a_k \cdot k(k-1) \cdots (k-i-1)) x^{k-i}$ Now since is a field k of characteristic 0, it contains a copy of \mathbb{Q} , so $\frac{1}{i!} g(x)$, for $g \in k[x]$ is well-defined for all $i \in \mathbb{N}$. Therefore:

$$\frac{D^{i}f(x)}{i!} = \sum_{k=i}^{n} a_{k} \frac{k(k-1)\cdots(k-i-1)}{i!} x^{k-i} = \sum_{k=i}^{n} a_{k} \frac{k(k-1)\cdots(k-i-1)(k-i)\cdot 1}{i!(k-i)!} x^{k-i} = \sum_{k=i}^{n} a_{k} \binom{k}{i} x^{k-i} = \varphi_{i}(x)$$
(10)

Exercise 4
Exercise 5

- (a) Show that $x^4 + 1$ and $x^6 + x^3 + 1$ are irreducible in \mathbb{Q}
- (b) Show that any polynomial of degree 3 in any field is either irreducible or has a root. Is $x^3 5x^2 + 1$ irreducible over \mathbb{Q} ?
- (c) Show that $x^2 + y^2 1$ is irred over \mathbb{Q} . Is it irred over \mathbb{C} ?
- (a) *Proof.* Let $f(x) = x^4 + 1$ and $g(x) = x^6 + x^3 + 1$. Note that:

$$f(x+1) = (x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$$
(1)

Note since 2 divides the coefficients of all x^i , for i < 4 and $2^2 = 4 \nmid 2$, by the Eisenstein criterion, f(x+1) is irreducible, therefore since we have a clear automorphism $\mathbb{Q}[x] \to \mathbb{Q}[x]$ given by $x \to (x+1)$ we see that f(x) is also irreducible.

Likewise we see that

$$g(x+1) = (x+1)^{6} + (x+1)^{3} + 1 = x^{6} + 6x^{5} + 15x^{4} + 21x^{3} + 18x^{2} + 9x + 3$$
(2)

Once again by the Eisenstein criterion with 3, g(x+1) is irreducible so f(x) is also irreducible.

(b) Assume that f(x) is a polynomial over a field k that is not irreducible, so $\exists g, h \in k[x]$ of positive degree such that:

$$f(x) = g(x)h(x) \Rightarrow 3 = \deg(f) = \deg(g) + \deg(h) \tag{3}$$

Since $\deg(g), \deg(h) > 0$, this means that $\deg(g) = 1$ and $\deg(h) = 2$ or vice-versa. Since a linear polynomial divides f, it has a root in k.

Let $f(x) = x^3 - 5x^2 + 1 \in \mathbb{Q}[x]$, assume that this polynomial has a root in \mathbb{Q} , say p/q, where $p, q \in \mathbb{Z}$, $\gcd(p, q) = 1$.

By the rational root theorem, we have that $p \mid 1$ and $q \mid 1$, therefore $p = \pm 1$ and $q = \pm 1$, so p/q = 1 or p/q = -1.

But notice that $f(1) = 1 - 5 + 1 = -3 \neq 0$ and $f(-1) = -1 - 5 + 1 = 5 \neq 0$. So in all cases $f(p/q) \neq 0$, which contradicts our assumption that p/q was a root of f.

Therefore, f(x) has no roots in \mathbb{Q} and so it is irreducible.

(c) Let $f(x,y) = x^2 + y^2 - 1$, we will show that this polynomial is irreducible over \mathbb{C} which will imply it is also irreducible over \mathbb{Q} .

Assume that f is not irreducible, so there exists $g, h \in \mathbb{C}[x.y]$ with $\deg(g), \deg(h) > 0$, such that f = gh.

By comparing degrees we immediately see that g, h are linear functions. Furthermore we can assume that the coefficient of x in these two polynomials is 1. Indeed since we have:

$$x^2 + y^2 - 1 = (ax + by + c)(dx + ey + f)$$
, by comparing coefficients $ad = 1$ (4)

$$\therefore x^{2} + y^{2} - 1 = \alpha d(x + \frac{b}{a}y + \frac{c}{a})(x + \frac{e}{d}y + \frac{f}{d})$$
 (5)

So we let $\alpha, \beta, \gamma, \epsilon \in \mathbb{C}$ such that $g(x, y) = x + \alpha y + \beta$ and $h(x, y) = x + \gamma y + \epsilon$ and:

$$f(x,y) = g(x,y)h(x,y) \tag{6}$$

$$x^2 + y^2 - 1 = (x + \alpha y + \beta)(x + \gamma y + \epsilon) \tag{7}$$

$$= x^{2} + (\alpha + \gamma)xy + (\alpha\gamma)y^{2} + (\epsilon + \beta)x + (\alpha\epsilon + \beta\gamma)y + \beta\epsilon$$
 (8)

By comparing coefficients we see that:

$$\begin{cases} \alpha + \gamma = 0 \\ \alpha \gamma = 1 \\ \epsilon + \beta = 0 \\ \alpha \epsilon + \beta \gamma = 0 \\ \beta \epsilon = -1 \end{cases} \Rightarrow \begin{cases} \alpha = -\gamma \\ \alpha^2 = -1 \Rightarrow \alpha \neq 0 \\ \epsilon = -\beta \\ -\alpha \beta - \beta \alpha = 0 \Rightarrow \alpha \beta = 0 \\ \beta^2 = 1 \Rightarrow \beta \neq 0 \end{cases}$$

But we have $\alpha, \beta \neq 0$ and $\alpha\beta = 0$ which is impossible. Therefore f(x, y) is irreducible over \mathbb{C} and \mathbb{Q} .

Exercise 8. Let A be a commutative entire ring (integral domain) and X a variable over A. Let $a, b \in A$ and assume that a is a unit in A. Show that the map $x \to ax + b$ extends to a unique automorphism of A[x] inducing the identity on A. What is the inverse automorphism?

Proof. Let $\varphi \colon \{x\} \subseteq A[x] \to A[x]$ be given by $\varphi(x) = (ax + b)$, and define $\bar{\varphi} \colon A[x] \to A[x]$ such that for all $f = \sum a_i x^i$:

$$\bar{\varphi}(f) = \bar{\varphi}(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} a_i \varphi(x)^i = \sum_{i=0}^{n} a_i (ax+b)^i = f(ax+b)$$
(9)

It is clear that this is a homomorphism, since we have

$$\bar{\varphi}(\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i) = \bar{\varphi}(\sum_{i=0}^{n} (a_i + b_i) x^i)$$
(10)

$$=\sum_{i=0}^{n}(a_i+b_i)\varphi(x)^i$$
(11)

$$= \sum_{i=0}^{n} a_i \varphi(x)^i + \sum_{i=0}^{n} b_i \varphi(x)^i$$
 (12)

$$= \bar{\varphi}(\sum_{i=0}^{n} a_i x^i) + \bar{\varphi}(\sum_{i=0}^{n} b_i x^i)$$

$$\tag{13}$$

And we have:

$$\bar{\varphi}\left(\sum_{i=0}^{n} a_i x^i \sum_{i=0}^{n} b_i x^i\right) = \bar{\varphi}\left(\sum_{0 \le i, j \le n} a_i b_j x^{i+j}\right)$$
(14)

$$= \bar{\varphi} \left(\sum_{k=0}^{n} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k \right) \tag{15}$$

$$= \sum_{k=0}^{n} \left(\sum_{i=0}^{k} a_{i} b_{k-i}\right) \varphi(x)^{k}$$
 (16)

$$= \sum_{k=0}^{n} \left(\sum_{i=0}^{k} a_i b_{k-i}\right) (ax+b)^k \tag{17}$$

$$= (\sum_{i=0}^{n} a_i (ax+b)^i) (\sum_{j=0}^{n} b_j (ax+b)^j)$$
(18)

$$= \bar{\varphi}(\sum_{i=0}^{n} a_i)\bar{\varphi}(\sum_{j=0}^{n} a_i) \tag{19}$$

Finally this induces the identity on A by definition, so $\bar{\varphi}(1) = 1$. Now if $f(x) = \sum_{i=0}^{n} a_i x^i \in \ker \bar{\varphi}$, then we have:

$$0 = \bar{\varphi}(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} a_i \varphi(x)^i$$
(20)

$$= \sum_{i=0}^{n} a_i (ax+b)^i$$
 (21)

$$= \sum_{i=0}^{n} \sum_{k=0}^{i} a_i \binom{i}{k} a^k b^{i-k} x^k \tag{22}$$

$$= \sum_{i=0}^{n} \left(a^{i} \sum_{k=i}^{n} a_{k} \binom{n}{k} b^{i-k}\right) x^{i}$$
 (23)

Therefore $a^i \sum_{k=i}^n a_k \binom{n}{k} b^{i-k} = 0$ for all i. But since $a \in A^*$, this means that $\sum_{k=i}^n a_k \binom{n}{k} b^{i-k} = 0 \ \forall i > 0$. We have two cases

- 1. If b = 0, then $\sum_{k=i}^{n} a_k \binom{n}{k} b^{i-k} = a_i = 0$ for all i.
- 2. If $b \neq 0$, and assume that $f \neq 0$, let i_0 be the largest i such that $a_i \neq 0$ then since:

$$0 = \sum_{k=i_0}^{n} a_k \binom{n}{k} b^{i_0 - k} = a_{i_0} \binom{n}{i_0} \Rightarrow a_{i_0} = 0$$
 (24)

Which is a contradiction to our assumption. So f = 0.

So this function is indeed 1-1. Now notice that

$$\bar{\varphi}(a^{-1}(x-b)) = a^{-1}(\bar{\varphi}(x-b)) = a^{-1}(\bar{\varphi}(x) - \bar{\varphi}(b)) = a^{-1}(ax+b-b) = x$$

By the fact that $\bar{\varphi}$ is a homomorphism, so for any $\sum a_i x^i \in A[x]$, we have:

$$\bar{\varphi}(\sum a_i(a^{-1}(x-b))^i) = \sum a_i\bar{\varphi}(a^{-1}(x-b))^i = \sum a_ix^i$$
 (25)

So this function is indeed onto, so $\bar{\varphi}$ is indeed an automorphism, inducing the identity on A. Furthermore, it is clearly the unique map extending φ since for any other map $\tilde{\varphi}$ extending φ we have:

$$\bar{\varphi}(\sum a_i x^i) = \sum a_i \bar{\varphi}(x)^i = \sum a_i \varphi(x)^i = \sum a_i \tilde{\varphi}(x)^i = \tilde{\varphi}(\sum a_i x^i)$$
(26)

From this it is clear that $\bar{\varphi}^{-1}$, is the unique automorphism extending $x \to a^{-1}(x-b)$, inducing the identity of A. Indeed call this automorphism $\bar{\psi}$, we have:

$$\bar{\varphi} \circ \bar{\psi}(\sum a_i x^i) = \sum a_i (\bar{\varphi} \circ \bar{\psi}(x))^i = \sum a_i (\bar{\varphi}(a^{-1}(x-b)))^i = \sum a_i x^i$$
(27)

Exercise 9. Show that every automorphism of A[x] is of the type described in Ex 8.

Proof.

Remark. Note, it is not written in my copy, but we need the automorphism to also induce the identity on A, since if not then the homomorphism $\phi \colon A[x][y] \to A[x][y]$, where $\phi(f(x,y)) = \phi(\sum f_i(x)y^i) = \sum f_i(y)x^i = f(y,x)$ is an automorphism but is not of the form in exercise 8.

Let $f = \sum a_i x^i$, be such that $\varphi(f) = x$, then we have:

$$\varphi(f) = \sum_{i=0}^{n} a_i \varphi(x)^i = x \tag{28}$$

Since we know that $\varphi(x) \notin A$, we see that $\deg(\varphi(x)^i) \geq i$. So by comparing degrees we see that $a_i = 0$ for all i > 1. So we have:

$$a_0 + a_1 \varphi(x) = x \tag{29}$$

Therefore we see that $\varphi(x)$ is linear, likewise we see that $\varphi^{-1}(x)$ is linear. So let $\varphi(x) = ax + b$ and $\varphi^{-1} = cx + d$ so we have:

$$x = \varphi^{-1}(\varphi(x)) \tag{30}$$

$$= c\varphi(x) + d \tag{31}$$

$$=c(ax+b)+d\tag{32}$$

$$= cax + (cb + d) \tag{33}$$

By comparing coefficients we see that ca=1, so a is a unit. So we indeed see that φ is of the form from Ex. 8.

Exercise 11. Let A be a commutative entire ring and K be it's quotient field. Let D: $A \to A$, be a derivation, an additive homomorphism s/t: D(xy) = xD(y) + yD(x)

(a) Prove that D has a unique extension to a derivation of K into itself and this extension satisfies the rule

$$D(x/y) = \frac{yDx - xDy}{y^2}, \text{ for } x, y \in A \text{ and } y \neq 0$$
(34)

Proof. We define $\bar{D}: K \to K$, by:

$$\bar{D}(x/y) = \frac{yDx - xDy}{y^2}, \text{ for all } x, y \in A \text{ with } y \neq 0$$
(35)

We will first show that this function is well-defined, let $\frac{x}{y} = \frac{z}{w} \iff xw = zy$, then we have:

$$\bar{D}(x/y) = \frac{yDx - xDy}{y^2} \tag{36}$$

$$\bar{D}(z/w) = \frac{wDz - zDw}{w^2} \tag{37}$$

We see that

$$w^{2}(yDx - xDy) = w^{2}yDx - w^{2}xDy$$

$$= w^{2}yDx - wzyDy$$

$$= yw(wDx - zDy)$$

$$= yw(D(wx) - xD(w) - D(yz) + yDz) \text{ by the product rule on } D$$

$$= yw(yD(z) - xD(w)) \text{ since } xw = zy$$

$$= y^{2}wD(z) - ywxD(w)$$

$$(38)$$

$$(40)$$

$$= yw(yDx - xD(w) - D(yz) + yDz) \text{ by the product rule on } D$$

$$= yw(yD(z) - xD(w)) \text{ since } xw = zy$$

$$= y^{2}wD(z) - ywxD(w)$$

$$(43)$$

$$= y^{2}wD(z) - y^{2}zD(w)$$

$$= y^{2}(wD(z) - zD(w))$$
(44)

Therefore $\bar{D}(x/y) = \bar{D}(z/w)$, this function is well-defined.

Now we will show that \bar{D} is a derivation. Let $\frac{x}{y}, \frac{z}{w} \in A$, not necessarly equal, we have:

$$\bar{D}\left(\frac{x}{y} + \frac{z}{w}\right) = \bar{D}\left(\frac{xw + zy}{yw}\right) \tag{46}$$

$$= \frac{ywD(xw + yz) - (xw + yz)D(yw)}{(yw)^2} \tag{47}$$

$$= \frac{ywD(xw) + ywD(yz) - xwD(yw) - yzD(yw)}{(yw)^2} \tag{48}$$

$$= \frac{yw(wDx + xDw) + yw(yDz + zDy) - xw(yDw + wDy) - yz(yDw + wDy)}{(yw)^2} \tag{49}$$

$$= \frac{yw^2Dx + (ywz - xw^2 - yzw)Dy + y^2wDz + (ywx - xwy - y^2z)Dw}{(yw)^2}$$
(50)

$$= \frac{w^2(yDx - xDy) + y^2(wDz - zDw)}{(yw)^2}$$
(51)

$$=\frac{yDx - xDy}{y^2} + \frac{wDz - zDw}{w^2} \tag{52}$$

$$= \bar{D}(x/y) + \bar{D}(z/w) \tag{53}$$

Likewise we see that:

$$\bar{D}\left(\frac{x}{y}\frac{z}{w}\right) = \bar{D}\left(\frac{xz}{yw}\right) \tag{54}$$

$$=\frac{ywD(xz) - xzD(yw)}{(yw)^2} \tag{55}$$

$$=\frac{yw(xDz+zDx)-xz(wDy+yDw)}{(yw)^2}$$
(56)

$$= \frac{yx(wDz - zDw) + wz(yDx - xDy)}{(yw)^2}$$

$$= \frac{x(wDz - zDw)}{w^2y} + \frac{z(yDx - xDy)}{y^2w}$$
(58)

$$=\frac{x(wDz-zDw)}{w^2y} + \frac{z(yDx-xDy)}{y^2w}$$
(58)

$$= \frac{x}{y}\bar{D}(\frac{z}{w}) + \frac{z}{w}\bar{D}(\frac{x}{y}) \tag{59}$$

Finally we see that for $x \in A$ we have:

$$\bar{D}(x) = \bar{D}(x/1) \tag{60}$$

$$=\frac{1D(x) - xD(1)}{1^2} \tag{61}$$

$$= Dx - xD(1) \tag{62}$$

But we also know that for all $x \in A$, $D(x) = D(1x) = xD(1) + 1D(x) \Rightarrow xD(1) = 0$. In particular this is true for x = 1, so D(1) = 0, so we indeed see that:

$$\bar{D}(x) = Dx$$
, for all $x \in A$ (63)

(b) Let L(x) = Dx/x, for $x \in K^*$. Show that L(xy) = L(x) + L(y), this is called the logarithmic derivative.

Proof.

$$L(xy) = D(xy)/xy (64)$$

$$=\frac{xDy+yDx}{xy}\tag{65}$$

$$=\frac{Dy}{y} + \frac{Dx}{x} \tag{66}$$

$$= L(x) + L(y) \tag{67}$$

(c) Let D be the standard derivative in k[x], over a field k. Let $R(x) = c\Pi(x - \alpha_i)^{m_i}$ with $\alpha_i, c \in k$ and $m_i \in \mathbb{Z}$. Show that:

$$R'/R = \sum \frac{m_i}{x - \alpha_i} \tag{68}$$

Proof. We use (a) to extend D to a derivative on k(x), we have:

$$R'/R = L(R) = L(c\Pi(x - \alpha_i)^{m_i}) = L(c) + \sum L((x - \alpha_i)^{m_i})$$
(69)

Recall that D(c) = 0, furthermore, if $m_i < 0$ then we have:

$$0 = D(1) \tag{70}$$

$$=D((x-\alpha_i)^{m_i}(x-\alpha_i)^{-m_i}) \tag{71}$$

$$= (x - \alpha_i)^{-m_i} D((x - \alpha_i)^{m_i}) + (x - \alpha_i)^{m_i} D((x - \alpha_i)^{-m_i})$$
(72)

$$= (x - \alpha_i)^{-m_i} D((x - \alpha_i)^{m_i}) - m_i (x - \alpha_i)^{m_i} (x - \alpha_i)^{-m_i - 1}$$
(73)

$$= (x - \alpha_i)^{-m_i} D((x - \alpha_i)^{m_i}) - m_i (x - \alpha_i)^{-1}$$
(74)

Therefore, $D((x - \alpha_i)^{m_i}) = m_i(x - \alpha_i)^{m_i-1}$, so the regular formula for D still words so we see that:

$$R'/R = \sum \frac{D(x - \alpha_i)^{m_i}}{(x - \alpha_i)^{m_i}} = \sum \frac{m_i(x - \alpha_i)^{m_i - 1}}{(x - \alpha_i)^{m_i}} = \sum \frac{m_i}{(x - \alpha_i)}$$
(75)