11. a) Prove that the kernel of the homomorphism $\varphi: \mathbb{C}[x, y] \to \mathbb{C}[t]$ defined by $x \mapsto t^2$, $y \mapsto t^3$ is the principal ideal generated by the polynomial $y^2 - x^3$.

Answer:

Let $I = (y^2 - x^3)$. We first show that $I \subseteq \ker \varphi$. Let $f = (y^2 - x^3)g(x, y) \in \mathbb{C}[x, y]$. $\varphi(f) = (t^6 - t^6)g(t^2, t^3) = 0$.

Next we show that $\ker \varphi \subseteq I$. First note that $\mathbb{C}[x, y] = \mathbb{C}[x][y]$. Let $f \in \ker(\varphi)$.

Using the division algorithm we have $f(x, y) = g(x, y)(y^2 - x^3) + h(x, y)$ where the degree of $h(x, y)$ in $y$ is less than 2. Thus, $h(x, y) = p(x) \cdot y + p'(x)$ where $p(x)$ and $p'(x) \in \mathbb{C}[x]$. Let $p(x) = \sum_{i=0}^{n} a_i x^i$ and $p'(x) = \sum_{i=1}^{m} b_i x^i$. Since $f(x, y) \in \ker \varphi$, we have

$$\varphi(f(x, y)) = \varphi(g(x, y)) \cdot \varphi(y^2 - x^3) + \varphi(h(x, y))$$

$$= 0 + \varphi(p(x)) \cdot t^3 + \varphi(p'(x))$$

$$= t^3 \sum_{i=0}^{n} a_i t^{2i} + \sum_{i=0}^{m} b_i t^{2i}$$

$$= \sum_{i=0}^{n} a_i t^{2i+3} + \sum_{i=0}^{m} b_i t^{2i} = 0$$

where $\theta$ is a constant polynomial. But $2i + 3$ is an odd integer for all $i$ while $2i$ is even. Hence for equation (1) to hold we must have $a_i = b_i = 0 \forall i$. So, $h(x, y) = 0$ and $f(x, y) = g(x, y)(y^2 - x^3) \subseteq I$.

b) Determine the image of $\varphi$ explicitly.

Answer:

By part (a) we have that for any $f(x, y) \in \mathbb{C}[x][y]$ $\varphi(f) = \sum_{i=0}^{n} a_i t^{2i+3} + \sum_{i=0}^{m} b_i t^{2i}$. Hence, $\varphi(f)$ can be any polynomials in $t$ with coefficient of $t^i = 0$, i.e. $\text{Im}(\varphi) = \left\{ \sum_{i=1}^{n} a_i t^i \mid a_i \in \mathbb{C} \right\}$. Constructively, let $n \in \mathbb{Z}$, then if $m = 2n \ (n \in \mathbb{Z})$, consider $x^n : \varphi(x^n) = t^{2n} = t^m$. If $m = 2n + 1 \ (n \in \mathbb{Z}, n \neq 0)$ then $\varphi(x^{n-1} y) = (t^2)^{n-1} t^3 = t^{2n+1}$.
**Question:**

20. Determine all automorphisms of the ring \( \mathbb{Z}[x] \).

**Answer:**

The set of all automorphisms \( \varphi: \mathbb{Z}[x] \to \mathbb{Z}[x] = \{ \varphi \mid \varphi(1) = 1 \text{ and } \varphi(x) = ax + b \text{ where } a = \pm 1, b \in \mathbb{Z} \} \).

First note that since \( \mathbb{Z}[x] \) is generated by 1, and \( x \) it is sufficient to give the image of 1 and \( x \) to completely determine \( \varphi \). Next, any automorphism from \( \mathbb{Z}[x] \to \mathbb{Z}[x] \) when reduced to \( \mathbb{Z} \) must be the identity (proposition 3.9). Thus, \( \varphi(1) = 1 \) and it remains to show that the only possibility are \( \varphi(x) = ax + b \) with \( a = \pm 1 \). First we see that if \( \varphi(x) = p(x) \), and the degree \( (p(x)) \geq 2 \) then \( \varphi \) is not surjective, for \( x \) has no pre-image.

Next, let \( \varphi(x) = ax + b \). Since \( \varphi \) must be an automorphism, then \( \exists p(x) \in \mathbb{Z}[x] \) such that \( \varphi(p(x)) = x \). Clearly, \( p(x) \) must be of degree 1, since \( \varphi(n) = n \), for all \( n \in \mathbb{Z} \). Thus,

\[
\varphi(cx + d) = \varphi(c)\varphi(x) + \varphi(d) = c(ax + b) + d = cax + cb + d
\]

which means that \( c a = 1 \) and \( a \) is a unit in \( \mathbb{Z} \). Hence, \( a = \pm 1 \).

So we are left to show that any map of the form \( \varphi(1) = 1 \) and \( \varphi(x) = ax + b \), for \( a = \pm 1, b \in \mathbb{Z} \) is a bijective map. Let \( \varphi^{-1}(x) = \pm(x - b) \) depending if \( a = \pm 1 \). Then \( \varphi \varphi^{-1} = \varphi^{-1}\varphi = id \) and \( \varphi \) is a bijection.

**Question:**

23. Let \( R \) be a ring of characteristic \( p \). Prove that if \( a \) is nilpotent then \( 1 + a \) is unipotent, that is, some power of \( 1 + a \) is equal to 1.

**Answer:**

Since the characteristic of \( R \) is \( p \), we have that \( \forall r \in R \ p \cdot r = p \cdot 1 \cdot r = 0 \cdot r = 0 \). Moreover for any \( n \in \mathbb{Z} \) such that \( p|n \) we also have that \( n \cdot r = 0 \). Assume that \( a \) is nilpotent and that \( n \) is the smallest positive integer such that \( a^n = 0 \). Since \( p \) is prime we have that \( p \left( j^p \right) \) for all \( 0 < j < p^k \). Since \( a^n = 0 \) for some \( n \geq 1 \), choose \( k \) such that \( p^k > n \), then \( (a + 1)^{p^k} = a^{p^k} + 1^{p^k} = a^{p^k-n} \cdot a^n + 1 = (a^{p^k-n}) \cdot 0 + 1 = 1 \).
Section 10.4

Question:
2 Determine the structure of the ring \( \mathbb{Z}[x]/(x^2 + 3, p) \), where (a) \( p = 3 \), (b) \( p = 5 \).

Answer:

a) First notice that the ideal \( (x^2 + 3, 3) = (x^2, 3) \). Thus in the quotient ring 
\[ \mathbb{Z}[x]/(x^2, 3) \], \( x^2 = 0 \) and \( 3 = 0 \). This means that the polynomials left have degree 1 with integer coefficients modulo 3. Hence, \( \mathbb{Z}[x]/(x^2, 3) = \{ax + b \mid a, b \in \mathbb{Z}_p\} \) with multiplication \((ax + b)(cx + d) = (ad + bc)x + bd \) where \( ad + bc = ad + bd \) (mod 3) and \( (bd) = bd \) (mod 3). In fact, \( \mathbb{Z}[x]/(x^2, 3) \approx \mathbb{Z}_3[x]/(x^2) \).

b) In a similar way \( \mathbb{Z}[x]/(x^2 + 3, 5) \approx \{ax + b / a, b \in \mathbb{Z}_5\} \) and multiplication given by 
\((ax + b)(cx + d) = acx^2 + (ad + bc)x + bd \) where \( x^2 = -3 = 2 \) and \( ac, (ad + bc), bd \) are residue mod 5.
Hence, \( \mathbb{Z}[x]/(x^2 + 3, 5) \approx \mathbb{Z}_5[\sqrt{2}] \).

Question:
3. Describe each of the following rings.

a) \( \mathbb{Z}[x]/(x^2 - 3, 2x + 4) \) (b) \( \mathbb{Z}[i]/(2 + i) \)

Answer:

a) Let \( \mathbb{Z}[x]/(x^2 - 3, 2x + 4) = R' \). In \( R' \), \( x^2 - 3 = 0 \) and \( 2x + 4 = 0 \)
\( \Rightarrow x^2 = 3 \) and \( 2x = -4 \).
Warning: We cannot conclude that \( x = -2 \) in \( R' \) because \( 2x + 4 = 2(x + 2) \) which means that both 2 and \( (x + 2) \) are zero divisors. But we can obtain 
\( 4x^2 = 16 \) and \( 4x^2 = 12 \Rightarrow 12 = 16 \Rightarrow 4 = 0 \), in \( R' \).

But we can do better:
\( x^2 - 3 + 2x + 4 = x^2 + 2x + 1 \Rightarrow 2x^2 + 4x + 2 \in I \) and 
\( 2x^2 + 4x + 2 - (x(2x + 4)) = 2 \) in \( I \). So, \( 2 \in I \) and \( x^2 - 3 + 4 = x^2 + 1 \in I \).

Also, we see that \( (x^2 - 3, 2x + 4) = (x^2 + 1, 2) \). Thus,
\( \mathbb{Z}[x]/(x^2 - 3, 2x + 4) = \mathbb{Z}[x]/(x^2 + 1, 2) \)
\( \approx \mathbb{Z}_2[x]/(x^2 + 1) \)
\( \approx \mathbb{Z}_2[i] \)

b) \( \mathbb{Z}[i]/(2 + i) = R' \) impose the relation \( i = -2 \) in \( R' \). But \( i^2 = -1 \), so \( i^2 = -1 = 4 \) and \( 5 = 0 \). Thus \( \mathbb{Z}[i]/(2 + i) \approx \mathbb{Z}_5 \).