Math 113, **Second Midterm Exam**
SOLUTIONS

(1) Part (a) is a special case of Exercise 20 in Section 26. We will check the two conditions in Definition 18.9 on page 171. First, since $\mathbf{Z}_3[x]$ is a commutative ring, we have

$$\phi(f(x)g(x)) \;=\; (f(x)g(x))^3 \;= f(x)^3 \cdot g(x)^3 \;= \phi(f(x)) \cdot \phi(g(x)).$$

Second, since $\mathbf{Z}_3[x]$ is a ring of characteristic 3, we have

$$\phi(f(x)+g(x)) \;=\; (f(x)+g(x))^3 \;=\; f(x)^3 + g(x)^3 \;=\; \phi(f(x)) + \phi(g(x)).$$

For part (b) we note that $\phi(f(x)) = f(x)^3 = f(x^3)$ can only be the zero polynomial when $f(x)$ itself is the zero polynomial. Hence the kernel of ϕ is the **zero ideal** $\langle 0 \rangle$ in $\mathbf{Z}_3[x]$.

(2) (a) We shall **prove** that the ring $R = \mathbf{Z}_3[x]\langle f(x) \rangle$ is a field. First, the polynomial $f(x) = x^3 + x^2 + 2$ has no zeros in $\mathbf{Z}_3$ because $f(0) = f(2) = 2$ and $f(1) = 1$. Theorem 23.10 on page 214 ensures that $f(x)$ is irreducible in $\mathbf{Z}_3[x]$. By Theorem 27.25 on page 251, the ideal $\langle f(x) \rangle$ is maximal in $\mathbf{Z}_3[x]$. Hence R is a field, by Theorem 27.9 on page 247.

(b) The field R is an extension of degree 3 over $\mathbf{Z}_3$. Thus R is a 3-dimensional vector space over $\mathbf{Z}_3$. By Theorem 33.1 on page 200, the field R has precisely $3^3 = \mathbf{27}$ elements.

(3) (a) The ideal $\langle y \rangle$ is non-zero and it is prime because $\mathbf{R}[x,y]/\langle y \rangle \simeq \mathbf{R}[x]$ is an integral domain. Moreover, $\langle y \rangle$ is not maximal because it is strictly contained in the ideal $\langle x, y \rangle$.
(b) The ideal $\langle x, y \rangle$ is not principal: it cannot be generated by one element because x and y have no common non-constant factor. It is maximal since $\mathbf{R}[x,y]/\langle x,y \rangle \simeq \mathbf{R}$ is a field.

(4) We fix the lexicographic term order with $x > y$. The two given generators of the ideal I have the underlined leading terms:

$$f(x,y) \;=\; \underline{\mathbf{x}} + \mathbf{y} \quad \text{and} \quad g(x,y) \;=\; \underline{x^2} + y^2 - 1.$$

Their S-polynomial $S(f,g) \;=\; xf(x,y) - g(x,y) \;=\; \underline{xy} - y^2 + 1$ reduces to $h(x,y) \;=\; S(f,g) - yf(x,y) \;=\; \underline{\mathbf{-2y^2}} + \mathbf{1}$ by one step of the Division Algorithm. By Theorem 26.6, the set $\mathcal{G} \;=\; \big\{ f(x,y),\, h(x,y) \big\}$ also generates I. We find that $\mathcal{G}$ is a Gröbner basis of I because $S(f,h) = 2yf(x,y) + h(x,y) = 2xy - 1$ reduces to zero by the Division Algorithm.

(b) The variety $V(I)$ consists of the **two points** $\big(-\frac{1}{\sqrt{2}}, +\frac{1}{\sqrt{2}}\big)$ and $\big(+\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\big)$.

(5) The assertion is the converse to Theorem 31.3 on page 283, and it is **false**, as seen in Exercise 19 (c) in Section 31. For a counterexample, let $F = \mathbf{Q}$ be the field of rational numbers and let $E = \overline{\mathbf{Q}}$ be its algebraic closure in the field of complex numbers $\mathbf{C}$. Then E is algebraic over F, by definition, but it is not a finite-dimensional vector space over F.