Partial HW11 Solutions

3.58 Find the gcd of $x^2 - x - 2$ and $x^3 - 7x + 6$ in $\mathbb{F}_5[x]$, and express it as a linear combination of them.
Solution. The Euclidean algorithm shows that

$$\gcd(x^2 - x - 2, x^3 - 7x + 6) = x - 2,$$

and

$$x - 2 = -\tfrac{1}{4}(x^3 - 7x + 6) + \tfrac{1}{4}(x + 1)(x^2 - x - 2).$$

3.66 If k is a field in which $1 + 1 \neq 0$, prove that $\sqrt{1 - x^2} \notin k(x)$, where $k(x)$ is the field of rational functions.
Solution. Suppose, on the contrary, that $\sqrt{1 - x^2} = f(x)/g(x)$, where $f(x), g(x) \in k[x]$; we may assume that $f(x)/g(x)$ is in lowest terms; that is, $f(x)$ and $g(x)$ are relatively prime. Cross multiply and square, obtaining

$$f(x)^2 = g(x)^2(1 - x^2) = g(x)^2(1 - x)(1 + x).$$

Since $1 + 1 \neq 0$, the polynomials $1 - x$ and $1 + x$ are relatively prime and irreducible, Euclid's lemma gives $1 - x \mid f(x)$ and $1 + x \mid f(x)$; that is,

$$f(x) = (1 - x^2)h(x)$$

for some $h(x) \in k[x]$. After substituting and canceling,

$$h(x)^2(1 - x^2) = g(x)^2.$$

Repeat the argument to obtain $1 - x \mid g(x)$, and this contradicts $f(x)$ and $g(x)$ being relatively prime. Therefore, $\sqrt{1 - x^2} \notin k(x)$.

3.75 If k is a field, show that the ideal (x, y) in $k[x, y]$ is not a principal ideal.
Solution. If the ideal (x, y) in $k[x, y]$ is a principal ideal, then there is $d = d(x, y)$ that generates it. Thus, $x = d(x, y)f(x, y)$ and $y = d(x, y)g(x, y)$ for $f(x, y), g(x, y) \in k[x, y]$. Taking degrees in each variable, $\deg_x(d) \leq 1$ and $\deg_y(d) \leq 1$, and so $d(x, y) = ax + by + c$, for some constant c. If x is a multiple of $ax + by + c$, then $b = 0$; if y is a multiple, then $a = 0$. We conclude that $d(x, y)$ is a nonzero constant. Since k is a field, d is a unit, and so $(x, y) = (d) = k[x, y]$, a contradiction.

3.81 Prove that there are domains R containing a pair of elements having no gcd.

Solution. Let k be a field, and let R be the subring of $k[x]$ consisting of all polynomials having no linear term; that is, $f(x) \in R$ if and only if $f(x) = s_0 + s_2x^2 + s_3x^3 + \cdots$. We claim that x^5 and x^6 have no gcd: their only monic divisors are 1, x^2, and x^3, none of which is divisible in R by the other two. For example, x^2 is not a divisor of x^3, for if $x^3 = f(x)x^2$, then (in $k[x]$) we have $\deg(f) = 1$. But there are no linear polynomials in R.