due April ~~8~~ 11

Homework Set 11
(section 4.4)

Name: _____

When writing a proof, be sure to cite all of the properties, theorems, corollaries, and definitions you use. Be sure to write all of your answers in complete sentences (even the non-proof questions).

1. Find the remainder when $f(x)$ is divided by $g(x)$.
   a. $f(x) = 2x^5 - 3x^4 + x^3 + 2x + 3$ and $g(x) = x - 3$ in $\mathbb{Z}_5[x]$

By the remainder theorem, the remainder when $f(x)$ is divided by $g(x)$ is $f(3) = 279 = 4$ in $\mathbb{Z}_5[x]$.

   b. $f(x) = 10x^{75} - 8x^{65} + 6x^{45} + 4x^{37} - 2x^{15} + 5$ and $g(x) = x + 1$ in $\mathbb{Q}[x]$

By the remainder theorem, the remainder when $f(x)$ is divided by $g(x)$ is $f(-1) = -10 + 8 - 6 - 4 + 2 + 5 = -5$ in $\mathbb{Q}[x]$.

2. For what value of k is $x + 1$ a factor of $x^4 + 2x^3 - 3x^2 + kx + 1$ in $\mathbb{Z}_5[x]$?

Using the remainder theorem and the factor theorem, we know $x+1$ is a factor of $f(x) = x^4 + 2x^3 - 3x^2 + kx + 1$ if and only if $f(-1) = 0$.
Here $f(-1) = 1 - 2 - 3 - k + 1 = -k - 3$. If $f(-1) = 0$, then $-k - 3 = 0$.
Hence if $k = -3$, $x+1$ is a factor of $f(x)$.
$\Rightarrow k = 2$

3. Let F be a field. If $f(x)$ and $g(x)$ are associates in $F[x]$, prove that the two polynomials have the same roots in F.

Let F be a field, and $g(x)$ and $f(x)$ are associates in $F[x]$.
By the definition of associates, there exists a unit $u(x)$ in $F[x]$ such that $f(x) = u(x)g(x)$. By Corollary 4.9, $u(x) = u$ where u is a unit in F.
Thus, $f(x) = u \cdot g(x)$. Suppose $r \in F$ is a root of $g(x)$. By the remainder theorem, we know r is a root of $g(x)$ means that $g(r) = 0_F$. Then $f(r) = u \cdot g(r) = u \cdot 0_F = 0_F$. Hence, r is also a root of $f(x)$. Now, suppose that $t \in F$ is a root of $f(x)$. By the remainder theorem, we know that $f(t) = 0_F$. Since $f(x) = u \cdot g(x)$, we get that $g(x) = u^{-1} \cdot f(x)$. u^{-1} exists because u is a unit. Then $g(t) = u^{-1} \cdot f(t) = u^{-1} \cdot 0_F = 0_F$.
Hence t is also a root of $g(x)$.
Thus, $f(x)$ and $g(x)$ have the same roots.

4. Find a prime $p > 5$ such that $x^2 + 1$ in reducible in $\mathbb{Z}_p[x]$.

$p = 13$

Let $x = 5$.

Then $x^2+1 = 25+1 = 26 = 0$ in $\mathbb{Z}_{13}$.

So $x^2+1 = (x+5)(x-5) = (x+5)(x+8)$

$p = 17$

Let $x = 4$

Then $x^2+1 = 16+1 = 17 = 0$ in $\mathbb{Z}_{17}$.

So $x^2+1 = (x-4)(x+4) = (x+4)(x+13)$

5. $\mathbb{Q}[\sqrt{2}]$ is the set of numbers of the form $r_0 + r_1\sqrt{2} + r_2(\sqrt{2})^2 + \cdots + r_n(\sqrt{2})^n$ where n is a non-negative integer and all of the $r_i \in \mathbb{Q}$.

a. Prove that $\mathbb{Q}[\sqrt{2}]$ is a subring of $\mathbb{R}$.

Obviously, $\mathbb{Q}[\sqrt{2}]$ is a subset of $\mathbb{R}$.

Let $r, t \in \mathbb{Q}[\sqrt{2}]$. Then $r = r_0 + r_1\sqrt{2} + \ldots + r_n(\sqrt{2})^n$ and $t = t_0 + t_1\sqrt{2} + \ldots + t_m(\sqrt{2})^m$.

Suppose $n \le m$. $r - t = (r_0 - t_0) + (r_1 - t_1)\sqrt{2} + \ldots + (r_n - t_n)(\sqrt{2})^n + \ldots + t_m(\sqrt{2})^m$.

Since $\mathbb{Q}$ is a ring, $r_i - t_i \in \mathbb{Q}$ for each i. Thus, $r - t \in \mathbb{Q}[\sqrt{2}]$.

$rt = r_0t_0 + (r_0t_1 + r_1t_0)\sqrt{2} + \ldots + r_nt_m(\sqrt{2})^{n+m}$. Since $\mathbb{Q}$ is a ring, $\sum_{i=0}^{k} r_i t_{k-i}$ is in $\mathbb{Q}$. Thus, $rt \in \mathbb{Q}[\sqrt{2}]$.

By theorem 3.6, $\mathbb{Q}[\sqrt{2}]$ is a subring of $\mathbb{R}$.

b. Prove that the function $\varphi: \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{2}]$ defined by $\varphi(f(x)) = f(\sqrt{2})$ is a surjective homomorphism, but not an isomorphism.

Let $\varphi: \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{2}]$ be a function defined by $\varphi(f(x)) = f(\sqrt{2})$.

Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{Q}[x]$. Then

$\varphi(f(x) + g(x)) = f(\sqrt{2}) + g(\sqrt{2}) = \varphi(f(x)) + \varphi(g(x))$ and

$\varphi(f(x)g(x)) = f(\sqrt{2})g(\sqrt{2}) = \varphi(f(x))\varphi(g(x))$.

Hence φ is a homomorphism.

Let $r \in \mathbb{Q}[\sqrt{2}]$. Then $r = r_0 + r_1\sqrt{2} + r_2(\sqrt{2})^2 + \ldots + r_n(\sqrt{2})^n$ for $n \ge 0$ and $r_i \in \mathbb{Q}$.

Define $f(x) = r_0 + r_1x + r_2x^2 + \ldots + r_nx^n$. Then $f(x) \in \mathbb{Q}[x]$, and $f(\sqrt{2}) = r$.

Thus, we see that φ is surjective.

φ is not injective because $f(x) = 1 + 3x + 5x$ and $g(x) = 11 + 3x$ will both get mapped to the same element in $\mathbb{Q}[\sqrt{2}]$. Namely,

$\varphi(f(x)) = 1 + 3\sqrt{2} + 5(\sqrt{2})^2 = 1 + 3\sqrt{2} + 10 = 11 + 3\sqrt{2} = \varphi(g(x))$.

But $f(x) \neq g(x)$.