Name: _____ Exam 2 - MAT513

Here are nine problems, 20 points each, straight from the text, for a total of 180 points. You may assume all rings are commutative and unital.

Problem 16.70. Let F be a field. Let $I = \{f(x) \in F[x] \mid f(a) = 0 \text{ for all } a \in F\}$. Show that I is an ideal of $F[x]$ and that I is infinite when F is finite and $I = \{0\}$ when F is infinite.

In any case, $I = \langle p(x) \rangle$. Suppose F is finite, then $p(x) = \prod_{a \in F}(x - a)$ and clearly I is infinite. If F is not finite, let $\{a_i\}_{i \in \mathbb{N}}$ be an infinite set of elements from F, then $p_n(x) = \prod_{i<n}(x - a_i) \in I$. If $p(x) \neq 0$ say $\deg(p(x)) = n$ we have $p(x) \mid p_n(x)$ and as $\deg(p(x)) = \deg(p_n(x))$ it must be that $p(x) = c \cdot p_n(x)$ for some $c \in F$. But then $p_n(a_n) = \prod_{i<n}(a_n - a_i) \neq 0$, since $a_n - a_i \neq 0$ and F in an integral domain. This contradicts the hypothesis, so $p(x) = 0$ must hold.

Problem 16.72. Let R be a ring, prove that $R[x]$ and $R[x^2]$ are isomorphic.

Let $\phi : R[x] \to R[x^2]$ be the obvious map extending the identity on R and $x \mapsto x^2$, namely, $\phi(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) = a_n = a_n x^{2n} + a_{n-1}x^{2(n-1)} + \cdots + a_0$. This is a homomorphism of the rings and is clearly 1-1 and onto.

Problem 17.10. Let $f(x) \in \mathbb{Z}_p[x]$ be irreducible and $\deg(f(x)) = n$, show that $\mathbb{Z}_p[x]/\langle f(x) \rangle$ is a field of size p^n.

From the Euclidean division algorithm we know $g(x) = f(x)q(x)+r(x)$ where $\deg(r(x)) < n$ so $r(x) = a_{n-1}x^{n-1} + \cdots + a_0$ and hence there are p^n many options for $(a_0, \cdots, a_{n-1})$ and hence p^n many elements of $\mathbb{Z}_p[x]/\langle f(x) \rangle$.

Problem 17.30. Show that for every integer $n > 1$ there are infinitely many monic irreducible $f(x) \in \mathbb{Q}[x]$ with $\deg(f(x)) = n$.

This is trivial from Eisenstein's criteria. Let p be a prime, then $f(x) = x^n + p$ is irreducible.

Problem 18.26. Show that every element of the form $(3 + 2\sqrt{2})^n$ is a unit in $\mathbb{Z}[\sqrt{2}]$.

$$(3 + 2\sqrt{2})^n(1 - 2\sqrt{2})^n = \left((3 + 2\sqrt{2})(3 - 2\sqrt{2})\right)^n = 1^n = 1$$

Problem 18.34. Show that in $\mathbb{Z}_5[x]$, $3x^2+4x+3 = (3x+2)(x+4) = (4x+1)(2x+3)$. Why does this not violate Theorem 18.3?

$$4x+1 = -x+1 = -(x-1) = -(x+4) \text{ and } 3x+2 = -2x-3 = -(2x+3)$$

So $4x+1$ and $x+4$ are associates as are $3x+2$ and $2x+3$.

Problem 18.44. Let F be a field and R be the subring of $F[x]$ generated by x^2 and x^3 and so that $F \subset R$, that is,

$$R = \bigcap \{D \subset F[x] \mid F \cup \{x^2, x^3\} \subset D \text{ and } D \text{ is a ring}\}.$$

Show that R is not a UFD.

Hint: Clearly, R is an integral domain since any subring of an integral domain is an integral domain. So the problem is unique factorization. Start by showing that x^2 and x^3 are irreducible in R. (You do need to **show** this!)

The elements of R are of the form $\sum_i a_{i,j}(x^2)^i(x^3)^j$, but any $n > 1$ can be written as $(2^{m_1} + \cdots 2^{m_k}) + 3$ where $m_i > 0$ (think about the binary representation of an integer) we see that $R = \{a_2x^2 + a_3x^3 + \cdots + a_nx^n \mid a_i \in F\} = x^2F[x]$. The only way to factor x^3 or x^2 would be to have x as a factor, and so x^2 and x^3 are irreducible. Clearly

$$x^6 = (x^2)^3 = (x^3)^2$$

Thus x^6 is representable in two distinct ways as a product of irreducibles. Hence, R is not a UFD.

Problem 19.34. Show that $f(x) = x^{19}+x^8+1$ has at least one repeated root in some extension of $\mathbb{Z}_3$.

$f'(x) = 19x^{18} + 8x^7 = x^{18} + 2x^7$. We see $f'(1) = f(1)$ so both have a factor of $(x-1)$; thus $f(x)$ has repeated roots in an extension.

Problem 19.38. Find the splitting field of $f(x) = x^4 - x^2 - 2$ over $\mathbb{Z}_3$.

$f(x) = (x^2-2)(x^2+1)$. x^2-2 and x^2+1 are irreducible over $\mathbb{Z}_3$. Either let $i = x+\langle x^2+1\rangle$ and $\mathbb{Z}_3(i) = \mathbb{Z}_3[x]/\langle x^2+1\rangle$ or just let $i = \sqrt{-1}$ and consider $\mathbb{Z}_3(i) = \{a+bi \mid a, b \in \mathbb{Z}_3\}$. Either way, this is a splitting field for x^2+1. Now x^2-2 is still irreducible over $\mathbb{Z}_3(i)$ and as above we have $\mathbb{Z}_3(i)(\sqrt{2}) = \mathbb{Z}_3(i)[x]/\langle x^2-2\rangle$, then this is a splitting field for $f(x)$ over $\mathbb{Z}_3$.