Math 307 Abstract Algebra Homework 12 **Name: Sample Solution.**

1. Show that the ideal $\langle x^2+1\rangle$ is prime in $\mathbb{Z}[x]$, but it is not a maximal ideal.

   Solution. For $A\langle x^2+1\rangle$ $\mathbb{Z}[x]/A = \{a+bx+A : a,b\in\mathbb{Z}\}$ is a commutative ring with unity $1+A$.

   If $a+bx+A$ and $c+dx+A$ satisfy $(a+bx+A)(c+dx+A) = (ac-bd)+(ad+bc)x+A$, and if $a+bx+A\neq 0$, then $ac-bd=0$ and $bc+ad=0$. For given $a+bx\neq 0$, the only solution for (c,d) is $(0,0)$. Thus, $\mathbb{Z}[x]/A$ has no zero divisors, and is an integral domain. Therefore, A is a prime ideal.

   Consider $f(x) = 2+A\in\mathbb{Z}[x]/A$. Then $(2+A)(a+bx+A) = 2a+2bx+A\neq 1+A$. Thus, $2+A$ has no inverse. Hence, $\mathbb{Z}[x]/A$ is not a field, and thus, it A is not a maximal ideal.

2. Suppose R is a commutative ring. Show that $R[x]$ and R have the same characteristics.

   Solution. Consider two cases.

   Case 1. $\text{char}(R) = m$ is finite. Then $ma=0$ for all $a\in R$. Thus, for any $f(x) = a_0+\cdots+a_nx^n$ we have $mf(x) = ma_0+\cdots+ma_nx^n = 0$. Furthermore, there is no smaller positive integer k such that $kf(x)=0$ for all $f(x)\in R[x]$, else, for any constant polynomial $f(x)=a$ we have $mf(x)=ma=0$, which contradicts the fact that $\text{char}(R)=m$.

   Case 2. $\text{char}(R)=0$. Then for any nonzero constant polynomial $f(x)=a$ we have $mf(x) = ma\neq 0$. So, $\text{char}(R)=0$.

3. Let $f(x) = a_0+\cdots+a_nx^n\in\mathbb{Z}[x]$. If $f(r/s)=0$, where $r/s\in\mathbb{Q}$ is in its lowest form, show that $r|a_0$ and $s|a_n$.

   Solution. If $0 = f(r/s) = a_0+a_1(r/s)+\cdots+a_n(r/s)^n$, then $s^na_0 = -r(a_1s^{n-1}+a_2rs^{n-2}+\cdots+a_nr^n)$. So, r is a factor of s^na_0. Since $\gcd(r,s)=1$, we see that $r|a_0$.

   Also, we have $r^na_n = -s(a_0s^{n-1}+a_1rs^{n-2}+\cdots+a_{n-1}r^{n-1})$. Thus, $s|a_n$.

4. Let $\mathbb{F}$ be a field, and $f(x) = f_0+\cdots+f_nx^n\in\mathbb{F}[x]$.

   (a) Show that $(x-1)$ is a factor of $f(x)$ if and only if $a_0+\cdots+a_n=0$.

   (b) Show that $(x+1)$ is a factor of $f(x)$ if and only if $a_0-a_1+\cdots+(-1)^na_n=0$.

   Solution. (a) By factor theorem, $0=f(1)=a_0+\cdots+a_n$.

   (b) By factor theorem, $0=f(-1)=a_0-a_1+a_2-\cdots+(-1)^na_n$.

5. Suppose $\mathbb{F}$ is a field, and $f(x),g(x)\in\mathbb{F}[x]$ are such that $f(a)=g(a)$ for infinitely many $a\in\mathbb{F}$. Show that $f(x)=g(x)$.

   Solution. Consider $h(x) = f(x)-g(x)$. If $h(x)$ is nonzero and has degree n, then $h(x)$ has at most n zeros. But $h(a) = f(a)-g(a)$ for infinitely many $a\in\mathbb{F}$. So, $h(x)=0$, and hence $f(x)=g(x)$.

6. (10 points) Let $\mathbb{F}$ be a field. For $f(x) = a_0+\cdots+a_nx^n\in\mathbb{F}[x]$, let

$$f'(x) = a_1+2a_2x+3a_3x^2+\cdots+na_nx^{n-1}.$$

(a) Prove that if $h(x) = f(x)g(x)$, then $h'(x) = f(x)g'(x) + f'(x)g(x)$.

(b) Show that a zero a of $f(x) \in \mathbb{F}[x]$ has multiplicity 2, i.e., $(x-a)^2$ is a factor of $f(x)$ if and only if a is a zero of $f(x)$ and a zero of $f'(x)$.

Solution. (a) Let $u(x) = u_0 + \cdots + u_n x^n$ and $v(x) = v_0 + \cdots + v_m x^m \in \mathbb{F}[x]$. We may assume that $n = m$ by adding $0x^j$ terms to the polynomial with lower degrees. Then $[u(x)+v(x)]' = (u_1+v_1) + 2(u_2+v_2)x + \cdots + n(u_n+v_n)x^{n-1} = v'(x) + v'(x)$.

Now, suppose $f(x), g(x) \in \mathbb{F}[x]$ has degree at most n. We the product rule by induction on n. For $n = 0$, the result is clear. Suppose the result is true for $f(x), g(x)$ of degrees up to n. Now, assume that $f(x)$ or / and $g(x)$ have degree $n+1$. Then $f(x) = f_1(x) + a_{n+1}x^{n+1}$ and $g(x) = g_1(x) + b_{n+1}x^{n+1}$. By induction assumption and the fact that $[u(x)+v(x)]' = u'(x) + v'(x)$, we have

$$\begin{aligned}
[f(x)g(x)]' &= [(f_1(x)g_1(x) + b_{n+1}x^{n+1}f_1(x) + a_{n+1}x^{n+1}g_1(x) + a_{n+1}b_{n+1}x^{2n+2}]' \\
&= f_1'(x)g_1(x) + f_1(x)g_1'(x) + (n+1)x^n b_{n+1}f_1(x) + x^{n+1}b_{n+1}f'(x) \\
&\quad +(n+1)x^n a_{n+1}g_1(x) + x^{n+1}a_{n+1}g_1'(x) + a_{n+1}b_{n+1}(2n+2)x^{2n+1} \\
&= [(n+1)a_{n+1}x^n + f_1'(x)][b_{n+1}x^{n+1} + g_1(x)] \\
&\quad +[a_{n+1}x^{n+1} + f_1(x)][(n+1)b_{n+1}x^n + g_1'(x)] \\
&= f'(x)g(x) + f(x)g'(x).
\end{aligned}$$

The result follows from the principle of MI.

Alternatively First, it is easy to show that the result holds if $f(x) = a_m x_m$. Second, it is easy to show that $(f_1(x) + f_2(x))' = f_1'(x) + f_2'(x)$. Consequently, the results holds for $f(x) = a_0 + \cdots + a_n x^n$.

(b) If $f(x) = (x-a)^2 g(x)$, then $f'(x) = 2(x-a)g(x) + (x-a)g'(x) = (x-1)[2g(x) + g'(x)]$. So, a is a zero for $f(x)$ and $f'(x)$.

Conversely, suppose a is a zero for $f(x)$ and $f'(x)$, then $f(x) = (x-a)g(x)$ and $f'(x) = g(x) + (x-a)g'(x)$. So, $f'(a) = 0$ implying that $g(a) = 0$. Thus, a is a zero of $g(x)$ and hence $f(x) = (x-a)g(x) = (x-a)^2 h(x)$ for some $h(x)$.

7. Find infinitely many polynomials $f(x)$ in $\mathbb{Z}_n[x]$ such that $f(a) = 0$ for all $a \in \mathbb{Z}_n$.

   Solution. Let $f(x) = x(x-1)\cdots(x-n+1)$. Then $f(x) = 0$ for all $a \in \mathbb{Z}_n$. Now, for any $g(x) \in \langle f(x)\rangle = \{f(x)h(x) : h(x) \in \mathbb{Z}_n[x]$, we have $g(a) = 0$ for all $a \in \mathbb{Z}_n$.

8. If $r \in \mathbb{R}$ such that $r + 1/r \in \mathbb{Z} \setminus \{2, -2\}$, than r is irrational.

   Solution. Suppose $r + 1/r = a \in \mathbb{Z} \setminus \{2, -2\}$, then r is a solution of $x^2 - ax + 1 = 0$. If $x = r/s$ is a solution with $r, s \in \mathbb{Z}$, then $r|1$ and $s|1$ by Problem 3. So, $r/s = \pm 1$. However, $x^2 - ax + 1 \neq 0$ for $x = \pm 1$ if $a \neq 2$.

9. Let $\mathbb{F}$ be a field. Show that there exist $a, b \in \mathbb{F}$ such that $x^2 + x + 1$ is a factor of $x^{43} + ax + b$.

   Solution 1. Divide x^{43} by $x^2 + x + 1$, we get $x^{43} = (x^2 + x + 1)g(x) - (ax + b)$ for some $a, b \in \mathbb{F}$.

Thus, $x^{43} + ax + b = (x^2 + x + 1)g(x)$.

Solution 2. One can actually shows that $x^{43} = (x^2 + x + 1)g(x) + x$. So, $(a, b) = (-1, 0)$.

10. (10 points) (Wilson's Theorem) In $\mathbb{Z}_n$, show that $(n-1)! = (n-1)$ if and only if n is a prime.

[Hint: Consider two cases: n is a prime, n is not a prime.]

Use this result to deduce the following.

(a) Find the remainder of 98! divided by 101.

(b) Show that $(50!)^2 = -1$ in $\mathbb{Z}_{101}$.

Solution. If n is a prime, then the nonzero elements $\mathbb{Z}_n$ is a cyclic group. Inverse elements in $\mathbb{Z}_n^*$ occur in pairs except for $a = 1, -1$. To, the product of the nonzero element will yield $-1 = n - 1$.

If n is not a prime, then the factor of n will be in $(n-1)!$ so that $(n-1)!$ is a multiple of n and equal to 0 in $\mathbb{Z}_n$.

(a) Note that 101 is a prime. In $\mathbb{Z}_{101}, 2 * 51 = 1$ so that $2^{-1} = 51$. Hence, $98!(99)(100) = 100! = -1$.

Thus, $98! = (-1)(-1)^{-1}(-2)^{-1} = -2^{-1} = -51 = 50$.

(b) In $\mathbb{Z}_{101}, [(50)!]^2 = (50)!(-51)(-52) \cdot (-100) = 100! = -1$.