Math 562/662 **Spring 2024**
Homework 4 **Drew Armstrong**

---

1. Extending Ring Homomorphisms to Polynomials. Given a ring homomorphism $\varphi : R \to S$ we define the function $\varphi : R[x] \to S[x]$ by sending $f(x) = \sum_k a_k x^k$ to

$$f^\varphi(x) := \sum_k \varphi(a_k)x^k.$$

(a) Prove that $f(x) \mapsto f^\varphi(x)$ is a ring homomorphism.

(b) Given an integer $n \geq 0$ let $\varphi : \mathbb{Z}[x] \to (\mathbb{Z}/n\mathbb{Z})[x]$ be the extension of the quotient homomorphism $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Show that

$$f^\varphi(x) = 0 \quad \Longleftrightarrow \quad n \text{ divides every coefficient of } f(x).$$

(c) **Gauss' Lemma.** A polynomial $f(x) \in \mathbb{Z}[x]$ is called *primitive* when its coefficients have no common prime factors. If $f(x), g(x) \in \mathbb{Z}[x]$ are primitive, prove that $f(x)g(x) \in \mathbb{Z}[x]$ is also primitive. [Hint: Let $p \geq 2$ be a common prime factor of the coefficients of $f(x)g(x)$ and let $\varphi : \mathbb{Z}[x] \to (\mathbb{Z}/p\mathbb{Z})[x]$ be the map from part (b). Since $\mathbb{Z}/p\mathbb{Z}$ is a field, and since $f^\varphi(x)g^\varphi(x) = \varphi(f(x)g(x)) = 0$ we must have $f^\varphi(x) = 0$ or $g^\varphi(x) = 0$.]

2. Equivalent Statements of the FTA. Consider the following statements:

(1$\mathbb{R}$) Every non-constant $f(x) \in \mathbb{R}[x]$ has a root in $\mathbb{C}$.
(2$\mathbb{R}$) Every non-constant $f(x) \in \mathbb{R}[x]$ is a product degree 1 and 2 polynomials in $\mathbb{R}[x]$
(1$\mathbb{C}$) Every non-constant $f(x) \in \mathbb{C}[x]$ has a root in $\mathbb{C}$.
(2$\mathbb{C}$) Every non-constant $f(x) \in \mathbb{C}[x]$ is a product of degree 1 polynomials in $\mathbb{C}[x]$.

I claim that these four statements are equivalent. We will prove the more difficult implications.

(a) Prove that (1$\mathbb{R}$) implies (2$\mathbb{R}$). [Hint: Let $* : \mathbb{C} \to \mathbb{C}$ be complex conjugation and let $* : \mathbb{C}[x] \to \mathbb{C}[x]$ be the extension as in Problem 1. For all $\alpha \in \mathbb{C}$ note that $f(\alpha)^* = f^*(\alpha^*)$. But if $f(x)$ has real coefficients then $f^*(x) = f(x)$. Use this to show that the non-real roots of a real polynomial come in complex conjugate pairs.]

(b) Prove that (1$\mathbb{R}$) implies (1$\mathbb{C}$). [Hint: Given $f(x) \in \mathbb{C}[x]$ we note that $(ff^*)^* = f^*(f^{**}) = f^*f = ff^*$, and hence the polynomial $f(x)f^*(x)$ has real coefficients. Assuming (1$\mathbb{R}$) we know that ff^* has a root $\alpha \in \mathbb{C}$, i.e., $f(\alpha)f^*(\alpha) = 0$. Use this to show that $f(x)$ has a root in $\mathbb{C}$.]

3. Freshman's Binomial Theorem. Let $p \geq 2$ be prime and let R be any ring of characteristic p. For any elements $a, b \in R$, prove that

$$(a + b)^p = a^p + b^p.$$

[Hint: For any $a \in R$ and $n \in \mathbb{Z}$ recall that we have an element $n \cdot a \in R$ defined by induction. If R has characteristic p then $p \cdot a = 0$ for any $a \in R$. For any $a, b \in R$, the usual binomial theorem for integers tells us that

$$(a + b)^p = a^p + \binom{p}{1} \cdot a^{p-1}b + \cdots + \binom{p}{p-1} \cdot ab^{p-1} + b^p.$$

Your job is to show that the integer $\binom{p}{k}$ is divisible by p whenever $1 \leq k \leq p - 1$.]

4. Eisenstein's Criterion. Let $p \geq 2$ be prime.

(a) Given a polynomial $f(x) = a_0 + \cdots + a_n x^n \in \mathbb{Z}[x]$ with $p|a_i$ for $0 \leq i \leq n-1$, $p \nmid a_n$ and $p^2 \nmid a_0$, prove that $f(x)$ is irreducible over $\mathbb{Z}$. [Hint: Suppose that $f(x) = g(x)h(x)$ with $\deg(g) = k \geq 1$ and $\deg(h) = \ell \geq 1$. Consider the ring homomorphism $\varphi : \mathbb{Z}[x] \to (\mathbb{Z}/p\mathbb{Z})[x]$ from 1(b), so that $g^\varphi(x)h^\varphi(x) = f^\varphi(x) = [a_n]x^n$ with $[a_n] \neq [0]$. Since p is prime this implies that $g^\varphi(x) = [b]x^k$ and $h^\varphi(x) = [c]x^\ell$ for some $[c], [d] \neq [0]$. But then the constant terms of $g(x)$ and $h(x)$ are divisible by p, so the constant term of $f(x) = g(x)h(x)$ is divisible by p^2.]

(b) The p-th cyclotomic polynomial is $\Phi_p(x) = 1 + x + \cdots + x^{p-1} = (x^p - 1)/(x - 1)$, so

$$\Phi_p(1+x) = \frac{(1+x)^p - 1}{x} = \binom{p}{1} + \binom{p}{2}x + \cdots + \binom{p}{p}x^{p-1}.$$

Use part (a) and the proof of Problem 3 to show that $\Phi_p(1+x)$ is irreducible over $\mathbb{Z}$. Use this to conclude that $\Phi_p(x)$ is irreducible over $\mathbb{Z}$.

5. Fundamental Theorem of Symmetric Polynomials. For any field $\mathbb{F}$, the symmetric group S_n acts on the set of polynomials $\mathbb{F}[x_1, \ldots, x_n]$ by permuting the variables:

$$\sigma \cdot f(x_1, \ldots, x_n) := f(x_{\sigma(1)}, \cdots, x_{\sigma(n)}).$$

We say that f is a *symmetric polynomial* when $\sigma \cdot f = f$ for all $\sigma \in S_n$.

(a) Let $\mathbf{x} = (x_1, \ldots, x_n)$. Then for any $\mathbf{k} = (k_1, \ldots, k_n) \in \mathbb{N}^n$ we define the notation

$$\mathbf{x}^\mathbf{k} := x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}.$$

Every $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ has a unique expression $f(\mathbf{x}) = \sum_{\mathbf{k} \in \mathbb{N}^n} a_\mathbf{k} \mathbf{x}^\mathbf{k}$ with $a_\mathbf{k} \in \mathbb{F}$ for all $\mathbf{k} \in \mathbb{N}^n$. Check that this notation satisfies $\mathbf{x}^\mathbf{k}\mathbf{x}^{\boldsymbol{\ell}} = \mathbf{x}^{\mathbf{k}+\boldsymbol{\ell}}$ for all $\mathbf{k}, \boldsymbol{\ell} \in \mathbb{N}^n$. It follows from this (but you don't need to prove it) that

$$\left(\sum_{\mathbf{k} \in \mathbb{N}^n} a_\mathbf{k} \mathbf{x}^\mathbf{k}\right)\left(\sum_{\boldsymbol{\ell} \in \mathbb{N}^n} b_{\boldsymbol{\ell}} \mathbf{x}^\ell\right) = \sum_{\mathbf{m} \in \mathbb{N}^n}\left(\sum_{\mathbf{k}+\boldsymbol{\ell}=\mathbf{m}} a_\mathbf{k} b_{\boldsymbol{\ell}}\right)\mathbf{x}^\mathbf{m}.$$

(b) We define the *lexicographic order* on $\mathbb{N}^n$ as follows:

$$\mathbf{k} < \boldsymbol{\ell} \quad \Leftrightarrow \quad \text{there exists } j \text{ such that } k_j < \ell_j \text{ and } k_i = \ell_i \text{ for all } i < j.$$

One can check (don't do this) that this defines a total order on $\mathbb{N}^n$ which satisfies the well-ordering property and for all $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{N}^n$ we have $\mathbf{a} \leq \mathbf{b} \Rightarrow \mathbf{a} + \mathbf{c} \leq \mathbf{b} + \mathbf{c}$. Based on this, we define the *lexicographic degree* function $\deg : \mathbb{F}[\mathbf{x}] \to \mathbb{N}^n$ by

$$\deg\left(\sum_{\mathbf{k} \in \mathbb{N}^n} a_\mathbf{k} \mathbf{x}^\mathbf{k}\right) := \max_{\text{lex}}\{\mathbf{k} \in \mathbb{N}^n : a_\mathbf{k} \neq 0\}.$$

Use part (a) and the given properties to show that $\deg(fg) = \deg(f) + \deg(g)$ for all nonzero polynomials $f(\mathbf{x}), g(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$.

(c) The *elementary symmetric polynomials* $e_1(\mathbf{x}), \ldots, e_n(\mathbf{x})$ are defined by

$$(y - x_1) \cdots (y - x_n) = y^n - e_1(\mathbf{x})y^{n-1} + e_2(\mathbf{x})y^{n-2} + \cdots + (-1)^n e_n(\mathbf{x}).$$

One can check that each $e_i(\mathbf{x})$ is monic (i.e., has lex-leading coefficient 1) and has $\deg(e_j) = (1, \ldots, 1, 0, \ldots, 0)$, with j ones followed by $n - j$ zeroes. For any symmetric polynomial $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$, prove that we can find a (possibly non-symmetric) polynomial $g(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ such that

$$f(\mathbf{x}) = g(e_1(\mathbf{x}), \ldots, e_n(\mathbf{x})).$$

[Hint: Use induction on lexicographic degree. Suppose that $f(\mathbf{x}) = c\mathbf{x}^{\mathbf{k}} +$ lower terms. Use the fact that $f(\mathbf{x})$ is symmetric to show that $k_1 \geq k_2 \geq \cdots \geq k_n$. Define

$$g(\mathbf{x}) := ce_1(\mathbf{x})^{k_1-k_2} e_2(\mathbf{x})^{k_2-k_3} \cdots e_{n-1}(\mathbf{x})^{k_{n-1}-k_n} e_n(\mathbf{x})^{k_n}$$

and use (b) to check that $g(\mathbf{x}) = c\mathbf{x}^{\mathbf{k}} +$ lower terms. Then since $\deg(f-g) < \deg(f)$ we may assume that $f(\mathbf{x}) - g(\mathbf{x}) = h(e_1(\mathbf{x}), \ldots, e_n(\mathbf{x}))$ for some $h(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$.]

(d) Let $f(x) \in \mathbb{F}[x]$ be a polynomial in one variable and let $\mathbb{E} \supseteq \mathbb{F}$ be a splitting field for $f(x)$ over $\mathbb{F}$. That is, suppose that there exist $\alpha_1, \ldots, \alpha_n \in \mathbb{E}$ such that

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n).$$

For any multivariable polynomial $F(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]$ we have the evaluation $F(\alpha_1, \ldots, \alpha_n) \in \mathbb{E}$. If F is symmetric, use part (c) to show that $F(\alpha_1, \ldots, \alpha_n) \in \mathbb{F}$.