MTH 562/662 **Spring 2019**
Exam 3 (Take Home) **Drew Armstrong**

Dedekind's Proof of the Irreducibility of $\Phi_n(x)$.

Problem 1. Gauss' Lemma. Given $f(x) = \sum_i a_i x^i \in \mathbb{Z}[x]$ we define the *content* as the greatest common divisor of the coefficients:

$$c(f) = c(a_0 + a_1 x + \cdots + a_n x^n) := \gcd(a_0, a_1, \ldots, a_n) \in \mathbb{N}.$$

(a) Let $d = \gcd(a_0, a_1, \ldots, a_n)$ with $a_i = da'_i$ for all i. Prove that $\gcd(a'_0, a'_1, \ldots, a'_n) = 1$.

Proof. Since d is a common divisor of the a_i we have $a_i = da'_i$ for some integers $a'_i \in \mathbb{Z}$. Now let $e \in \mathbb{N}$ be any common divisor of the a'_i, so that $a_i = ea''_i$ for some integers $a''_i \in \mathbb{Z}$. But then we have $a_i = (de)a''_i$ and hence de is a common divisor of the original a_i. Since d is the **greatest** common divisor we conclude that

$$\begin{aligned} de &\leq d \\ e &\leq 1. \end{aligned}$$

□

(b) If $f(x) \in \mathbb{Q}[x]$ is monic, prove that there exists an integer $k \in \mathbb{N}$ with $kf(x) \in \mathbb{Z}[x]$ and $c(kf) = 1$. [Hint: Choose any $n \in \mathbb{N}$ such that $nf(x) \in \mathbb{Z}[x]$ and let $d = c(nf)$.]

Proof. Suppose that $f(x) \in \mathbb{Q}[x]$ is monic and let $n \in \mathbb{N}$ be the product of the denominators of the coefficients, so that $nf(x) \in \mathbb{Z}[x]$. Now let $d = c(nf)$, so from part (a) we have $c\left(\frac{n}{d} f\right) = 1$. On the other hand, since d divides every coefficient of $nf(x)$ we have $\frac{n}{d} f(x) \in \mathbb{Z}[x]$ and since n is the leading coefficient of $nf(x)$ — indeed, $f(x)$ is monic — we conclude that $d|n$ and hence $k := n/d \in \mathbb{Z}$. □

(c) For all $f(x), g(x) \in \mathbb{Z}[x]$ prove that $c(f) = c(g) = 1$ implies $c(fg) = 1$. [Hint: For any prime p we know that f and g each have a coefficient not divisible by p. Show that fg also has a coefficient not divisible by p.]

Gauss' Proof.[1] Suppose that $f(x) = \sum a_i x^i$ and $g(x) = \sum b_j x^j$. If $c(f) = c(g) = 1$ then for any prime p there exists a smallest i such that $p \nmid a_i$ and a smallest j such that $p \nmid b_j$. Now let $k := i + j$ and consider the coefficient of x^k in the product $f(x)g(x)$:

$$a_0 b_{i+j} + \cdots + a_{i-1} b_{j+1} + a_i b_j + a_{i+1} b_{j-1} + \cdots + a_{i+j} b_0.$$

By assumption p divides every term except $a_i b_j$, hence it follows that p does not divide the whole sum. In other words, there exists a coefficient of $f(x)g(x)$ that is not divisible by p. Since this is true for any prime p be conclude that $c(fg) = 1$. □

---

[1] Article 42 of the *Disquisitiones*.

Modern Proof. Let p be prime and let $f(x) \mapsto \bar{f}(x)$ be the ring homomorphism $\mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$ defined by reducing each coefficient mod p. Since $c(f) = c(g) = 1$ we have $\bar{f}(x) \neq 0$ and $\bar{g}(x) \neq 0$. Then since $\mathbb{Z}/p\mathbb{Z}[x]$ is an integral domain we have

$$\overline{fg}(x) = \bar{f}(x)\bar{g}(x) \neq 0,$$

which implies that $f(x)g(x)$ has a coefficient not divisible by p. □

(d) If $f(x), g(x) \in \mathbb{Q}[x]$ are **monic** with $f(x)g(x) \in \mathbb{Z}[x]$, prove that $f(x), g(x) \in \mathbb{Z}[x]$. [Hint: From (b) we have $k, \ell \in \mathbb{N}$ with $kf(x), \ell g(x) \in \mathbb{Z}[x]$ and $c(kf) = c(\ell g) = 1$. Use (c) to show that $k\ell = 1$.]

Proof. Let $f(x), g(x) \in \mathbb{Q}[x]$ be monic with $f(x)g(x) \in \mathbb{Z}[x]$. From (b) we have $k, \ell \in \mathbb{N}$ such that $kf(x), \ell g(x) \in \mathbb{Z}[x]$ and $c(kf) = c(\ell g) = 1$. Then from (c) we have $c((kf)(\ell g)) = c((k\ell)(fg)) = 1$. Since every coefficient of $k\ell f(x)g(x) \in \mathbb{Z}[x]$ is divisible by $k\ell$ we conclude that $k\ell = 1$. It follows that $k = \ell = 1$ and hence $f(x), g(x) \in \mathbb{Z}[x]$.

□

Problem 2. Two More Lemmas. Let p be prime and let $f(x) \mapsto \bar{f}(x)$ denote the ring homomorphism $\mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$ defined by reducing each coefficient mod p.

(a) For any polynomial $g(x) \in \mathbb{Z}[x]$ show that $\bar{g}(x^p) = \bar{g}(x)^p$. [Hint: Frobenius.]

Proof. Since $\mathbb{Z}/p\mathbb{Z}[x]$ is is a ring of characteristic p we know that the function $\alpha \mapsto \alpha^p$ defines a ring homomorphism $\mathbb{Z}/p\mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$, called the Frobenius endomorphism. Furthermore, if $\bar{g}(x) = \sum a_i x^i \in \mathbb{Z}/p\mathbb{Z}[x]$ then from Fermat's Little Theorem we have $a_i^p = a_i$ for all p. It follows that

$$\bar{g}(x^p) = \sum a_i (x^p)^i = \sum (a_i x^i)^p = \sum \varphi(a_i x^i) = \varphi\left(\sum a_i x^i\right) = \bar{g}(x)^p.$$

□

(b) If p is prime and $p \nmid n$ show that $x^n - 1$ has no repeated factor in $\mathbb{Z}/p\mathbb{Z}[x]$. [Hint: Any repeated factor is also a factor of the derivative.]

Proof. Suppose that $x^n - 1 = f(x)^2 g(x)$ for some polynomials $f(x), g(x) \in \mathbb{Z}/p\mathbb{Z}[x]$. Then we have $D(x^n - 1) = f(x)\,[2Df(x)g(x) + f(x)Dg(x)]$, so that $f(x)$ is a common factor of $x^n - 1$ and $D(x^n - 1)$. On the other hand, we know that $D(x^n - 1) = nx^{n-1} \in \mathbb{Z}/p\mathbb{Z}[x]$. If $p \nmid n$ and hence $n \neq 0 \in \mathbb{Z}/p\mathbb{Z}$ then this implies that the only factors of $D(x^n - 1)$ are powers of x. But no power of x divides $x^n - 1$. □

Problem 3. The Proof. Let $\omega = e^{2\pi i/n}$ and recall that $\Phi_n(x) = \prod(x - \omega^k)$, where the product is over $0 \leq k < n$ such that $\gcd(k, n) = 1$. You proved on the homework that $\Phi_n(x)$ has integer coefficients. Now you will prove that $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.

(a) Let $\Phi_n(x) = f(x)g(x)$ with $f(x), g(x) \in \mathbb{Q}[x]$ monic and $f(x)$ irreducible. In this case prove that $f(x), g(x) \in \mathbb{Z}[x]$. [Hint: Problem 1.]

Proof. This follows immediately from 1(d). $\square$

(b) Suppose that $f(\omega^k) = 0 \Rightarrow f(\omega^{kp}) = 0$ for all $\gcd(k, n) = 1$ and for all primes $p \nmid n$. In this case prove that $f(x) = \Phi_n(x)$ and hence $\Phi_n(x)$ is irreducible. [Hint: Show that $f(\omega^\ell) = 0$ for all $\gcd(\ell, n) = 1$.]

Proof. For any $\gcd(k, n) = 1$ we have $f(\omega^k)g(\omega^k) = \Phi_n(\omega^k) = 0$ and hence $f(\omega^k) = 0$ or $g(\omega^k) = 0$. If $g(\omega^k) = 0$ for all $\gcd(k, n) = 1$ then from Descartes' Factor Theorem we would have $g(x) = \Phi_n(x)$, which contradicts the fact that $f(x)$ is irreducible. Therefore we must have $f(\omega^k) = 0$ for **some** $\gcd(k, n) = 1$.

In this case I claim that we also have $f(\omega^\ell) = 0$ for **all** $\gcd(\ell, n) = 1$. Indeed, since k, ℓ are coprime to n there exists some $\gcd(m, n) = 1$ such that $km = \ell \bmod n$. Furthermore, since $\gcd(m, n) = 1$ we can factor $m = p_1 \cdots p_r$ into primes such that $p_i \nmid n$ for all i. Then by repeatedly applying the supposition we conclude that

$$f(\omega^k) = 0 \Rightarrow f(\omega^{kp_1}) = 0 \Rightarrow \cdots \Rightarrow f(\omega^{kp_1 \cdots p_r}) = f(\omega^{km}) = 0 \Rightarrow f(\omega^\ell) = 0.$$

It follows from Descartes' Factor Theorem that $f(x) = \Phi_n(x)$. $\square$

(c) Otherwise we must have $f(\omega^k) = 0$ and $g(\omega^{kp}) = 0$ for some $\gcd(k, n) = 1$ and some prime $p \nmid n$. In this case prove that $g(x^p) = f(x)h(x)$ for some $h(x) \in \mathbb{Z}[x]$. [Hint: Show that $f(x)$ is the minimal polynomial of ω^k over $\mathbb{Q}$.]

Proof. Let $G(x) = g(x^p) \in \mathbb{Z}[x]$. Since $f(\omega^k) = 0$ with $f(x)$ monic and irreducible in $\mathbb{Q}[x]$ we know that $f(x)$ is the minimal polynomial for $\omega^k/\mathbb{Q}$. Then since $G(\omega^k) = 0$ we know that $f(x)|G(x)$ in $\mathbb{Q}[x]$, say $G(x) = f(x)h(x)$ for some $h(x) \in \mathbb{Q}[x]$. Finally, since $G(x), f(x) \in \mathbb{Z}[x]$ we conclude by uniqueness of quotients that $h(x) \in \mathbb{Z}[x]$. $\square$

(d) It follows from 2(a) that $\bar{f}(x)\bar{h}(x) = \bar{g}(x)^p$ in $\mathbb{Z}/p\mathbb{Z}[x]$. Use the fact that $\mathbb{Z}/p\mathbb{Z}[x]$ is a UFD to prove that $\bar{f}(x)$ and $\bar{g}(x)$ have a common factor in $\mathbb{Z}/p\mathbb{Z}[x]$.

Proof. Thus from 2(a) we have $\bar{f}(x)\bar{h}(x) = \bar{g}(x)^p$ in $\mathbb{Z}/p\mathbb{Z}[x]$. Since $\mathbb{Z}/p\mathbb{Z}$ is a field we know that $\mathbb{Z}/p\mathbb{Z}[x]$ is a UFD. It follows that any irreducible factor of $\bar{f}(x)$ in $\mathbb{Z}/p\mathbb{Z}[x]$ is also a factor of $\bar{g}(x)$. $\square$

(e) Use (d) to show that $x^n - 1$ has a multiple factor in $\mathbb{Z}/p\mathbb{Z}[x]$, contradicting 2(b).

Proof. But then $x^n - 1 = \prod_{d|n} \bar{\Phi}_d(n) = \bar{f}(x)\bar{g}(x) \cdot \prod_{d|n, d \neq n} \bar{\Phi}_d(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ has a multiple factor in $\mathbb{Z}/p\mathbb{Z}[x]$, contradicting 2(b). It follows that the situation of 3(b) must hold, and hence the cyclotomic polynomial $\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$. $\square$