Math 562/662 **Spring 2019**
Homework 4 **Drew Armstrong**

---

1. Computing Minimal Polynomials. Define $\alpha := \sqrt[3]{2} \in \mathbb{R}$ and $\omega := e^{2\pi i/3} \in \mathbb{C}$.

(a) Prove that $x^3 - 2$ is the minimal polynomial for α over $\mathbb{Q}(\omega)$.
(b) Prove that $x^2 + x + 1$ is the minimal polynomial for ω over $\mathbb{Q}(\alpha\omega)$.
(c) Prove that $x^2 + (\alpha\omega)x + (\alpha\omega)^2$ is the minimal polynomial for α over $\mathbb{Q}(\alpha\omega)$.

[Hint: Consider any $\beta \in \mathbb{E} \supseteq \mathbb{F}$ and let $f(x) \in \mathbb{F}[x]$ be a polynomial satisfying $\deg(f) = [\mathbb{E}/\mathbb{F}]$. Suppose also that $f(x)$ is monic and satisfies $f(\beta) = 0$, hence $m_{\beta/\mathbb{F}}(x) | f(x)$. Then since $m_{\beta/\mathbb{F}}(x)$ and $f(x)$ are monic of the same degree we conclude that $m_{\beta/\mathbb{F}}(x) = f(x)$.]

2. Repeated Roots. If $\mathbb{F}$ is a field then we can think of the ring of polynomials $\mathbb{F}[x]$ as an infinite dimensional $\mathbb{F}$-vector space with basis $\{1, x, x^2, \ldots\}$. Let $D : \mathbb{F}[x] \to \mathbb{F}[x]$ be the unique $\mathbb{F}$-linear function defined by

$$D(x^n) = nx^{n-1} \text{ for all } n \geq 0.$$

(a) For all polynomials $f(x), g(x) \in \mathbb{F}[x]$ prove that the *product rule* holds:

$$D(fg) = f \cdot Dg + Df \cdot g.$$

[Hint: Show that each side is an $\mathbb{F}$-bilinear function of f and g. Thus it suffices to check the case when $f = x^m$ and $g = x^n$ are basis elements.]

(b) Consider a polynomial $f(x) \in \mathbb{F}[x]$ and a field extension $\mathbb{E} \supseteq \mathbb{F}$. We say that $\alpha \in \mathbb{E}$ is a *repeated root* of f when $f(x) = (x - \alpha)^2 g(x)$ for some polynomial $g(x) \in \mathbb{E}[x]$. Use part (a) to prove that

$$\alpha \text{ is a repeated root of } f \quad \Longleftrightarrow \quad f(\alpha) = 0 \text{ and } Df(\alpha) = 0.$$

3. Cyclotomic Polynomials. Fix an integer n and consider the polynomial $x^n - 1 \in \mathbb{Z}[x]$.

(a) Factor $x^n - 1$ into irreducible polynomials over $\mathbb{C}$. [Hint: Let $\omega := e^{2\pi/n}$.]
(b) Factor $x^n - 1$ into irreducible polynomials over $\mathbb{R}$. [Hint: For all integers $k \in \mathbb{Z}$ we have $\omega^k + \omega^{-k} = 2\cos(2\pi k/n)$.]
(c) We define the n-th *cyclotomic polynomial* $\Phi_n(x) \in \mathbb{C}[x]$ as follows:

$$\Phi_n(x) := \prod_{\omega \in \Omega'_n} (x - \omega) \quad \text{where} \quad \Omega'_n := \{e^{2\pi i k/n} : 0 \leq k < n, \gcd(k, n) = 1\}.$$

Prove that

$$x^n - 1 = \prod_{d|n} \Phi_d(x) = \prod_{d|n} \Phi_{n/d}(x).$$

[Hint: The elements of Ω'_n are called the *primitive* nth roots of unity. Prove that the set of **all** nth roots of unity can be expressed as a disjoint union $\coprod_{d|n} \Omega'_d$.]

(d) Use part (c) and induction to prove that actually $\Phi_n(x) \in \mathbb{Z}[x]$. [Hint: For any $f(x), g(x) \in \mathbb{Z}[x]$ with $g(x)$ monic there exist **unique** polynomials $q(x), r(x) \in \mathbb{Z}[x]$ such that $f(x) = q(x)g(x) + r(x)$ and $\deg(r) < \deg(g)$.]

4. Impossible Constructions. We say that a number $\alpha \in \mathbb{R}$ is *constructible over* $\mathbb{Q}$ if there exists a chain of field extensions

$$\alpha \in \mathbb{F}_k \supseteq \mathbb{F}_{k-1} \supseteq \cdots \supseteq \mathbb{F}_1 \supseteq \mathbb{F}_0 = \mathbb{Q}$$

such that $[\mathbb{F}_{i+1}/\mathbb{F}_i] = 2$ for all i. [Reason: A point of $\mathbb{R}^2$ is "constructible with straightedge and compass" if and only if both of its coordinates are constructible in the above sense. This follows from the fact that intersections of lines and circles are solutions to quadratic equations.]

(a) Let $f(x) \in \mathbb{Q}[x]$ be any polynomial of degree 3. Prove that

$$f \text{ has a constructible root } \alpha \in \mathbb{R} \quad \Longrightarrow \quad f \text{ has a root in } \mathbb{Q}.$$

[Hint: You proved the induction step on the previous homework.]

(b) Prove that the real numbers $\sqrt[3]{2}$, $\cos(2\pi/18)$ and $\cos(2\pi/7)$ are not constructible. It follows from this that the classical problems of "doubling the cube," "trisecting the angle," and "constructing the regular heptagon" are impossible. [Hint: Show that each is a root of some irreducible polynomial $f(x) \in \mathbb{Q}[x]$ of degree 3.]

5. Primitive Root Theorem. If $\mathbb{F}$ is a finite field then the group of units $\mathbb{F}^\times$ is cyclic.

(a) Consider $m, n \in \mathbb{Z}$ with $\gcd(m, n) = 1$. If $m|nk$ for some $k \in \mathbb{Z}$, prove that $m|k$. If $m|k$ and $n|k$ for some $k \in \mathbb{Z}$ prove that $mn|k$. [Hint: Write $mx + ny = 1$.]

(b) Let A be an abelian group. If elements $a, b \in A$ have orders m, n with $\gcd(m, n) = 1$, prove that ab has order mn. [Hint: Show that $(ab)^k = \varepsilon$ implies $m|k$ and $n|k$.]

(c) Let A be an abelian group. If m is the **maximal order** of an element, prove that every element has order dividing m. [Hint: Let $a, b \in A$ have orders ℓ, m with $\ell \nmid m$. Then for some prime p we have $\ell = p^i\ell'$ and $m = p^j m'$ with $p \nmid \ell', m'$ and $i > j$. Use (b) to show that $a^{\ell'} b^{p^j}$ has order greater than m.]

(d) If $\alpha \in \mathbb{F}^\times$ is an element of **maximal order** m, prove that $\mathbb{F}^\times = \{1, \alpha, \ldots, \alpha^{m-1}\}$. [Hint: If not then the polynomial $x^m - 1 \in \mathbb{F}[x]$ has too many roots. Use (c).]

6. Laplace's Proof of the FTA. The FTA is easily proved with complex analysis. However, it is still nice to have an elementary proof that is mostly algebraic. The following proof from Laplace (1795) builds on earlier ideas of Euler (1749) and Lagrange (1770). A logical gap in the proof was later filled by Kronecker's Theorem (1887). Specifically, we will prove that

every non-constant polynomial $f(x) \in \mathbb{R}[x]$ has a root in $\mathbb{C}$.

(a) Observe that every polynomial $f(x) \in \mathbb{R}[x]$ of odd degree has a root in $\mathbb{R}$.

(b) Now let $f(x) \in \mathbb{R}[x]$ have degree $n = 2^e m$ with $e \geq 1$ and m odd. Consider $f(x)$ as an element of $\mathbb{C}[x]$ and let $\mathbb{E} \supseteq \mathbb{C}$ be a splitting field:

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) \in \mathbb{E}[x].$$

Now for any real number $\lambda \in \mathbb{R}$ we define the polynomial

$$g_\lambda(x) := \prod_{1 \leq i < j \leq n} (x - \beta_{ij\lambda}) \in \mathbb{E}[x] \quad \text{with} \quad \beta_{ij\lambda} := \alpha_i + \alpha_j + \lambda\alpha_i\alpha_j \in \mathbb{E}.$$

Prove that $g_\lambda(x) \in \mathbb{R}[x]$ and $\deg(g_\lambda) = 2^{e-1}m'$ with m' odd. [Hint: Newton.]

(c) By induction on e we can assume that $g_\lambda(x)$ has a complex root $\beta_{ij\lambda} \in \mathbb{C}$. If we apply this argument for more than $\binom{n}{2}$ different values of $\lambda \in \mathbb{R}$ then we will find specific indices $i < j$ and real numbers $\lambda \neq \mu$ such that $\beta_{ij\lambda}$ and $\beta_{ij\mu}$ are **both** in $\mathbb{C}$. In this case prove that α_i and α_j are in $\mathbb{C}$, hence $f(x)$ has a complex root.