Math 461 **Spring 2023**
Homework 5 **Drew Armstrong**

---

1. The Minimal Polynomial. This problem is a generalization of Descartes' Theorem. Consider a field extension $\mathbb{E} \supseteq \mathbb{F}$ and an element $\gamma \in \mathbb{E}$. Let $p(x) \in \mathbb{F}[x]$ be a prime polynomial satisfying $p(\gamma) = 0$.

(a) For all $f(x) \in \mathbb{F}[x]$, prove that

$$f(\gamma) = 0 \quad \Longleftrightarrow \quad f(x) = p(x)g(x) \text{ for some } g(x) \in \mathbb{F}[x].$$

[Hint: Let $f(\gamma) = 0$. If $p(x) \nmid f(x)$ then $p(x)$ and $f(x)$ are coprime in $\mathbb{F}[x]$, hence there exist $p'(x), f'(x) \in \mathbb{F}[x]$ satisfying $p(x)p'(x) + f(x)f'(x) = 1$. Now what?]

(b) If $q(x) \in \mathbb{F}[x]$ is another prime polynomial satisfying $q(\gamma) = 0$, use part (a) to show that $q(x) = cp(x)$ for some constant $c \in \mathbb{F}$. It follows that **there exists a unique monic, prime polynomial** $p(x) \in \mathbb{F}[x]$ **satisfying** $p(\gamma) = 0$, which we call *the minimal polynomial of* γ *over* $\mathbb{F}$.

(c) If $a \in \mathbb{F}$, what is the minimal polynomial of a over $\mathbb{F}$?

(d) What is the minimal polynomial of $\sqrt{-1}$ over $\mathbb{R}$?

(e) What is the minimal polynomial of $\omega = \exp(2\pi i/3)$ over $\mathbb{R}$?

2. Adjoining an Element to a Field. Let $p(x) \in \mathbb{F}[x]$ be the minimal polynomial for some element $\gamma \in \mathbb{E} \supseteq \mathbb{F}$ and suppose that $\deg(p) = d$. Consider the set of evaluations of all polynomials $f(x) \in \mathbb{F}[x]$ at $x = \gamma$, which is a subset of $\mathbb{E}$:

$$\mathbb{F}[\gamma] = \{f(\gamma) : f(x) \in \mathbb{F}[x]\} \subseteq \mathbb{E}.$$

It is easy to check that $\mathbb{F}[\gamma]$ is a subring of $\mathbb{E}$.

(a) Prove that

$$\mathbb{F}[\gamma] = \{a_0 + a_1\gamma + \cdots + a_{d-1}\gamma^{d-1} : a_0, a_1 \ldots, a_{d-1} \in \mathbb{F}\}.$$

[Hint: Every element $\alpha \in \mathbb{F}[\gamma]$ has the form $\alpha = f(\gamma)$ for some $f(x) \in \mathbb{F}[x]$. Divide $f(x)$ by $p(x)$ to get $f(x) = p(x)q(x) + r(x)$ for $q(x), r(x) \in \mathbb{F}[x]$ with $\deg(r) < d$.]

(b) Let $a_0, a_1, \ldots, a_{d-1}, b_0, b_1, \ldots, b_{d-1} \in \mathbb{F}[x]$ and define elements $\alpha, \beta \in \mathbb{F}[\gamma]$ by

$$\alpha = a_0 + a_1\gamma + \cdots + a_{d-1}\gamma^{d-1} \quad \text{and} \quad \beta = b_0 + b_1\gamma + \cdots + b_{d-1}\gamma^{d-1}.$$

Prove that $\alpha = \beta$ if and only if $a_i = b_i$ for all i. [Hint: Consider the polynomials $f(x) = a_0 + a_1x + \cdots + a_{d-1}x^{d-1}$ and $g(x) = b_0 + b_1x + \cdots + b_{d-1}x^{d-1}$ and let $h(x) = f(x) - g(x)$. Since $h(\gamma) = 0$, Problem 1(a) implies that $p(x)|h(x)$. Use this to show that $h(x) = 0$ and hence $f(x) = g(x)$, as desired.]

(c) Show that $\mathbb{F}[\gamma]$ is actually a **field**. [Hint: A general element $\alpha \in \mathbb{F}[\gamma]$ has the form $\alpha = f(\gamma)$ for some $f(x) \in \mathbb{F}[x]$. If $\alpha \neq 0$ then part (b) implies that $f(x) \neq 0$ and Problem 1(a) implies that $p(x) \nmid f(x)$. Since $p(x)$ is prime this means that $f(x)$ and $p(x)$ are coprime in $\mathbb{F}[x]$, hence there exist $f'(x), p'(x) \in \mathbb{F}[x]$ satisfying $f(x)f'(x) + p(x)p'(x) = 1$.]

3. Quadratic Field Extensions. Computing inverses in a field extension $\mathbb{F}[\gamma]$ involves the Extended Euclidean Algorithm. However, if the minimal polynomial of γ over $\mathbb{F}$ is quadradic then there is a shortcut called "rationalizing the denominator". Let $p(x) = x^2 + ux + v \in \mathbb{F}[x]$ be the minimal polynomial of γ and define the *conjugation function* $* : \mathbb{F}[\gamma] \to \mathbb{F}[\gamma]$ by

$$(a + b\gamma)^* = (a - ub) - b\gamma.$$

(a) For all $\alpha \in \mathbb{F}[\gamma]$ show that $\alpha = \alpha^*$ if and only if $\alpha \in \mathbb{F}$.

(b) For all $\alpha, \beta \in \mathbb{F}[\gamma]$ show that $(\alpha+\beta)^* = \alpha^* + \beta^*$ and $(\alpha\beta)^* = \alpha^*\beta^*$.

(c) Use the fact that $p(x) = x^2 + xu + v \in \mathbb{F}[x]$ is **prime** to show that $u^2 - 4v$ has no square root in $\mathbb{F}$. [Hint: Quadratic formula. More precisely, if $r \in \mathbb{F}$ and $r^2 = u^2 - 4v$, show that $(-u+r)/2 \in \mathbb{F}$ is a root of $p(x)$.]

(d) Given $\alpha \in \mathbb{F}[\gamma]$, it follows from (a) and (b) that $\alpha\alpha^* \in \mathbb{F}$. More precisely, we define the *norm function* $N : \mathbb{F}[\gamma] \to \mathbb{F}$ by

$$N(a + b\gamma) := (a+b\gamma)(a+b\gamma)^* = a^2 - abu + b^2 v \in \mathbb{F}.$$

For all $\alpha \in \mathbb{F}[\gamma]$, use part (c) to show that $\alpha \neq 0$ implies $N(\alpha) \neq 0$. [Hint: Consider a nonzero element $\alpha = a + b\gamma \neq 0$ and assume for contradiction that $N(\alpha) = 0$. If $b = 0$, use the fact that $N(\alpha) = 0$ to show that $a = 0$, contradicting the fact that $\alpha \neq 0$. If $b \neq 0$, use the fact that $N(\alpha) = 0$ to show that $\left(\frac{2a-bu}{b}\right)^2 = u^2 - 4v$, contradicting (c).]

(e) Given a nonzero element $\alpha = a + b\gamma \neq 0$, "rationalize the denominator" to find an explicit formula for $(a+b\gamma)^{-1}$.

4. The Rational Root Test.

(a) Consider integers $a, b, c \in \mathbb{Z}$ with $\gcd(a,b) = 1$. Prove that $a|bc$ implies $a|c$. [Hint: If $\gcd(a,b) = 1$ then $ax + by = 1$ for some $x, y \in \mathbb{Z}$. Multiply both sides by c.]

(b) Consider an integer polynomial $f(x) = c_n x^n + \cdots + c_1 x + c_0 \in \mathbb{Z}[x]$ and suppose that $f(x)$ has a rational root $a/b \in \mathbb{Q}$ with $\gcd(a,b) = 1$. In this case, use part (a) to show that $a|c_0$ and $b|c_n$. [Hint: Multiply both sides of $f(a/b) = 0$ by b^n to clear denominators.]

5. Constructible Numbers of Degree Three.

(a) Consider a quadratic field extension $\mathbb{F}[\gamma] \supseteq \mathbb{F}$ as in Problem 3, with conjugation map $* : \mathbb{F}[\gamma] \to \mathbb{F}[\gamma]$. For any polynomial $f(x) \in \mathbb{F}[x]$ of degree 3, prove that

$$f(x) \text{ has a root in } \mathbb{F}[\gamma] \quad \Longrightarrow \quad f(x) \text{ has a root in } \mathbb{F}.$$

[Hint: Suppose that $f(\alpha) = 0$ for some $\alpha \in \mathbb{F}[\gamma]$. If $\alpha \in \mathbb{F}$ then we are done. Otherwise, show that $f(\alpha^*) = 0$, and use this to show that $f(x) = (x-\alpha)(x-\alpha^*)g(x)$ for some polynomial $g(x) \in \mathbb{F}[x]$ of degree 1. You have done this before.]

(b) We showed in class that a real number $\alpha \in \mathbb{R}$ is *constructible with ruler and compass* if and only if it is contained in a chain of quadratic field extensions over $\mathbb{Q}$:

$$\alpha \in \mathbb{F}_n \supseteq \cdots \supseteq \mathbb{F}_2 \supseteq \mathbb{F}_1 \supseteq \mathbb{F}_0 := \mathbb{Q}.$$

Given a rational polynomial $f(x) \in \mathbb{Q}[x]$ of degree 3, use part (a) to prove that

$$f(x) \text{ has a constructible root} \quad \Longrightarrow \quad f(x) \text{ has a root in } \mathbb{Q}.$$

[Hint: Note that $f(x) \in \mathbb{F}_k[x]$ for all k. If $f(x)$ has a root in $\mathbb{F}_{k+1}$ then part (a) implies that $f(x)$ has a root in $\mathbb{F}_k$.]

6. Impossible Constructions. If a real number $\alpha \in \mathbb{R}$ satisfies $f(\alpha) = 0$ for some rational polynomial $f(x) \in \mathbb{Q}[x]$ of degree 3 with no rational roots, then Problem 5 implies that α **is not constructible**. We will apply this result and the rational root test to prove that the following real numbers not constructible:

$$\sqrt[3]{2}, \quad 2\cos\left(\frac{2\pi}{7}\right), \quad 2\cos\left(\frac{\pi}{9}\right).$$

(a) Show that the polynomial $x^3 - 2 \in \mathbb{Q}[x]$ has no rational root.

(b) Show that $\alpha = 2\cos(2\pi/7)$ is a root of the polynomial $x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$ and show that this polynomial has no rational root. [Hint: $\alpha = \omega + \omega^{-1}$ where $\omega = \exp(2\pi i/7)$.]

(c) Show that $\alpha = 2\cos(\pi/9)$ is a root of the polynomial $x^3 - 3x - 1 \in \mathbb{Q}[x]$ and show that this polynomial has no rational root. [Hint: Use de Moivre's identity $(\cos\theta + i\sin\theta)^3 = \cos(3\theta) + i\sin(3\theta)$ to show that

$$\cos(3\theta) = 4\cos^3\theta - 3\cos\theta,$$

then substitute $\theta = \pi/9$.]