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 $\mathbb{R}$?

(a): If $f(x) = p(x)g(x)$ for some $g(x) \in \mathbb{F}[x]$ then we have

$$f(\gamma) = p(\gamma)g(\gamma) = 0g(\gamma) = 0.$$

Conversely, we will show that $f(\gamma) = 0$ implies $p(x)|f(x)$ in the ring $\mathbb{F}[x]$. To do this, assume that $f(\gamma) = 0$ and suppose for contradiction that $p(x) \nmid f(x)$. Since $p(x)$ is a prime element in the Euclidean domain $\mathbb{F}[x]$ this implies that $\gcd(p, f) = 1$, hence from the Extended Euclidean Algorithm we can find some polynomials $p'(x), f'(x) \in \mathbb{F}[x]$ satisfying $p(x)p'(x) + f(x)f'(x) = 1$. Now substitute $x = \gamma$ to get the desired contradiction:

$$\begin{aligned} p(x)p'(x) + f(x)f'(x) &= 1 \\ p(\gamma)p'(\gamma) + f(\gamma)f'(\gamma) &= 1 \\ 0 &= 1. \end{aligned}$$

(b): Consider two polynomials $p(x), q(x) \in \mathbb{F}[x]$ satisfying the following properties:

- $p(x)$ and $q(x)$ are monic (i.e., have leading coefficient 1),
- $p(x)$ and $q(x)$ are prime elements of $\mathbb{F}[x]$,
- $p(\gamma) = 0$ and $q(\gamma) = 0$.

Applying part (a) with $f(x) = q(x)$ gives $p(x)|q(x)$. But the definitions of $p(x)$ and $q(x)$ are symmetric, so we also have $q(x)|p(x)$. For elements a, b in a domain R, recall that

$$a|b \text{ and } b|a \quad \Longleftrightarrow \quad a = ub \text{ for some unit } u \in R.$$

And recall that the units of the domain $\mathbb{F}[x]$ are the nonzero constants. It follows that $p(x) = cq(x)$ for some nonzero zero constant $c \in \mathbb{F}$, and since $p(x)$ and $q(x)$ are monic we must have $c = 1$.

Remark: Suppose that an "imaginary number" γ satisfies some polynomial equation $f(\gamma) = 0$ over a field of "real numbers" $\mathbb{F}$.[1] In this case we have shown that there exists a **unique** polynomial $p(x) \in \mathbb{F}[x]$ satisfying

[1] A number that satisfies a polynomial equation over a field $\mathbb{F}$ is called *algebraic over* $\mathbb{F}$. Some numbers do not satisfy polynomial equations. For example, the number $\pi \approx 3.14$ does not satisfy any polynomial equation

- $p(x)$ is monic,
- $p(x)$ is prime over $\mathbb{F}$,
- $p(\gamma) = 0$.

We call $p(x)$ the *minimal polynomial of* γ *over* $\mathbb{F}$. This definition is relative to the base field. For example, we will see below that the minimal polynomial over i over $\mathbb{R}$ is $x^2 + 1$, while the minimal polynomial of i over $\mathbb{C}$ is $x - i$.

(c): Given an element $a \in \mathbb{F}$ I claim that $p(x) = x - a \in \mathbb{F}[x]$ is the minimal polynomial. Indeed, this polynomial is monic, prime and satisfies $p(a) = 0$.

Remark: For all $f(x) \in \mathbb{F}[x]$ it follows from (a) that $f(a) = 0$ if and only if $f(x) = (x-a)g(x)$ for some $g(x) \in \mathbb{F}[x]$. This is just Descartes' Theorem.

(d): I claim that $p(x) = x^2 + 1 \in \mathbb{R}[x]$ is the minimal polynomial of i over $\mathbb{R}$. Indeed $p(x)$ is monic and satisfies $p(i) = (i)^2 + 1 = -1 + 1 = 0$. To see that $x^2 + 1$ is prime over $\mathbb{R}$, suppose that $x^2 + 1 = f(x)g(x)$ for some nonconstant polynomials $f(x), g(x) \in \mathbb{R}[x]$. By comparing degrees we must have $\deg(f) = \deg(g) = 1$. But then $x^2 + 1$ must have a real root, which is a contradiction.

Remark: For all $f(x) \in \mathbb{R}[x]$ it follows that $f(i) = 0$ if and only if $f(x) = (x^2 + 1)g(x)$ for some $g(x) \in \mathbb{R}[x]$.

(e): Note that $\omega = e^{2\pi i/3}$ is a root of the polynomial $x^3 - 1 \in \mathbb{R}[x]$. But this polynomial is not prime because

$$x^3 - 1 = (x - 1)(x^2 + x + 1).$$

Substituting $x = \omega$ into this factorization gives

$$0 = \omega^3 - 1 = (\omega - 1)(\omega^2 + \omega + 1),$$

which implies that $\omega^2 + \omega + 1 = 0$ because $\omega - 1 \neq 0$. I claim that $p(x) = x^2 + x + 1$ is the minimal polynomial of ω over $\mathbb{R}$. To see this, it only remains to show that $p(x)$ is prime over $\mathbb{R}$. And since $p(x)$ has degree 2 this follows from the fact that $p(x)$ has no roots in $\mathbb{R}$.

Remark: For all $f(x) \in \mathbb{R}[x]$ it follows that $f(\omega) = 0$ if and only if $f(x) = (x^2 + x + 1)g(x)$ for some $g(x) \in \mathbb{R}[x]$.

Remark: In parts (d) and (e) we used the fact that a polynomial $f(x) \in \mathbb{F}[x]$ of degree 2 is prime if and only if it has no root in $\mathbb{F}[x]$. This also holds for polynomials of degree 3. Indeed, let $\deg(f) = 3$ and suppose that $f(x) = g(x)h(x)$ for some nonconstant $g(x), h(x) \in \mathbb{F}[x]$. By comparing degrees we have $3 = \deg(f) = \deg(g) + \deg(h)$ which implies that $\deg(g) = 1$ or $\deg(h) = 1$. If $\deg(g) = 1$ then $g(x) = a + bx$ for some $a, b \in \mathbb{F}$ with $b \neq 0$ and it follows that $-a/b \in \mathbb{F}$ is a root of $f(x)$. Similarly, if $\deg(h) = 1$ then $f(x)$ has a root in $\mathbb{F}$. Summary: **If** $f(x) \in \mathbb{F}[x]$ **has degree two or three**, then

$$f(x) \text{ is prime over } \mathbb{F} \quad \Longleftrightarrow \quad f(x) \text{ has no roots in } \mathbb{F}.$$

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 $\mathbb{E}$:

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

over $\mathbb{Q}$, so we say that π *is transcendental over* $\mathbb{Q}$. This notion is relative to the base field. For example, π is transcendental over $\mathbb{Q}$ but it is algebraic over $\mathbb{R}$ with minimal polynomial $x - \pi \in \mathbb{R}[x]$.

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 $f(x)f'(x) + p(x)p'(x) = 1$.]

To emphasize: We assume that $p(x) \in \mathbb{F}[x]$ is the minimal polynomial of γ over $\mathbb{F}$ and that $\deg(p) = d$.

(a): By definition, every element $\alpha \in \mathbb{F}[\gamma]$ has the form $\alpha = f(\gamma)$ for some polynomial $f(x) \in \mathbb{F}[x]$. Divide $f(x)$ by $p(x)$ to get $f(x) = p(x)q(x) + r(x)$ where $q(x), r(x) \in \mathbb{F}[x]$ and $r(x) = 0$ or $\deg(r) < \deg(p) = d$. In any case we can write $r(x) = a_0 + a_1x + \cdots + a_{d-1}x^{d-1}$ for some coefficients $a_0, a_1, \ldots, a_{d-1} \in \mathbb{F}[x]$. But then

$$\begin{aligned}
\alpha &= f(\gamma) \\
&= p(\gamma)q(\gamma) + r(\gamma) \\
&= 0q(\gamma) + r(\gamma) \\
&= r(\gamma) \\
&= a_0 + a_1\gamma + \cdots + a_{d-1}\gamma^{d-1},
\end{aligned}$$

as desired.

(b): Consider any elements $\alpha, \beta \in \mathbb{F}[x]$. From part (a) we know that $\alpha = f(\gamma)$ and $\beta = g(\gamma)$ for some polynomials

$$\begin{aligned}
f(x) &= a_0 + a_1 + \cdots + a_{d-1}x^{d-1}, \\
g(x) &= b_0 + b_1 + \cdots + b_{d-1}x^{d-1},
\end{aligned}$$

with $a_0, \ldots, a_{d-1}, b_0, \ldots, b_{d-1} \in \mathbb{F}$. I claim that

$$\alpha = \beta \quad \Longleftrightarrow \quad a_i = b_i \text{ for all } i.$$

One direction is easy. For the other direction, consider the polynomial $h(x) = f(x) - g(x) \in \mathbb{F}[x]$. Since $h(\gamma) = f(\gamma) - g(\gamma) = \alpha - \beta = 0$, we know from 1(a) that $p(x)|h(x)$. I claim that this implies $h(x) = 0$. Indeed, if $h(x) \neq 0$ then the relation $p(x)|h(x)$ gives a contradiction:

$$d = \deg(p) \leq \deg(h) \leq \min\{\deg(f), \deg(g)\} \leq d - 1.$$

It follows that $f(x) = g(x)$ in the ring $\mathbb{F}[x]$ hence these polynomials have the same coefficients.

(c): To see that $\mathbb{F}[\gamma]$ is a field, consider any nonzero element $\alpha \in \mathbb{F}[\gamma]$. By definition we have $\alpha = f(\gamma)$ for some $f(x) \in \mathbb{F}[x]$. Since $\alpha \neq 0$, it follows from the easy direction of 1(a) that $p(x) \nmid f(x)$.[2] Then since $p(x)$ is a prime element of the Euclidean domain $\mathbb{F}[x]$ we have $\gcd(p, f) = 1$ and we can use the Extended Euclidean Algorithm to find polynomials $p'(x), f'(x) \in \mathbb{F}[x]$ satisfying $p(x)p'(x) + f(x)f'(x) = 1$. Now substitute $x = \gamma$ to obtain

$$\begin{aligned} p(x)p'(x) + f(x)f'(x) &= 1 \\ p(\gamma)p'(\gamma) + f(\gamma)f'(\gamma) &= 1 \\ 0p'(\gamma) + f(\gamma)f'(\gamma) &= 1 \\ f(\gamma)f'(\gamma) &= 1 \\ \alpha f'(\gamma) &= 1. \end{aligned}$$

Since $f'(\gamma) \in \mathbb{F}[\gamma]$, it follows that α^{-1} exists in $\mathbb{F}[\gamma]$.

Remark: The field $\mathbb{F}[\gamma]$ is completely analogous to the field $\mathbb{Z}/p\mathbb{Z}$ for a prime integer $p \in \mathbb{Z}$. Indeed, if $p(x)$ is the minimal polynomial of γ over $\mathbb{F}$ then for all polynomials $f(x), g(x) \in \mathbb{F}[x]$ we can define the notation

$$f(x) \equiv g(x) \mod p(x) \iff p(x) | (f(x) - g(x)).$$

And it follows from Problem 1a that

$$f(x) \equiv g(x) \mod p(x) \Leftrightarrow f(\gamma) = g(\gamma).$$

So the theory of field extensions is analogous to the theory of modular arithmetic. It gets really fun when you combine the two theories to obtain the theory of finite fields.

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

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

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 $(a + b\gamma)^{-1}$.

[2] In the hint I suggested to use 2(b). Actually it's much easier than this.

To emphasize: We assume that $p(x) = x^2 + ux + v \in \mathbb{F}[x]$ is the minimal polynomial of γ over $\mathbb{F}$, so each element $\alpha \in \mathbb{F}[\gamma]$ has a unique representation of the form $\alpha = a + b\gamma$ for some $a, b \in \mathbb{F}$. This uniqueness implies that $\gamma \notin \mathbb{F}$.

(a): Let $\alpha = a + b\gamma$ with $a, b \in \mathbb{F}$. Note that $\alpha \in \mathbb{F}$ if and only if $b = 0$. Indeed, if $\alpha = c \in \mathbb{F}$ and $b \neq 0$ then $\gamma = (c - a)/b \in \mathbb{F}$. Contradiction. Now we will show that $\alpha^* = \alpha$ if and only if $b = 0$. For the first direction, let $b = 0$. Then

$$\alpha^* = (a - bu) - b\gamma = (a - 0) - 0\gamma = a = a + 0\gamma = \alpha.$$

Conversely, suppose that $\alpha^* = \alpha$:

$$(a - bu) - b\gamma = a + b\gamma.$$

Comparing imaginary parts gives $b = -b$, hence $b = 0$.

(b): Given $\alpha = a + b\gamma$ and $\beta = c + d\gamma$ we have

$$\begin{aligned} \alpha^* &= (a - bu) - b\gamma, \\ \beta^* &= (c - du) - d\gamma, \end{aligned}$$

so that

$$\begin{aligned} (\alpha + \beta)^* &= [(a + c) + (b + d)\gamma]^* \\ &= [(a + c) - (b + d)u)] - (b + d)\gamma \\ &= [(a - bu) - b\gamma] + [(c - du) - d\gamma] \\ &= \alpha^* + \beta^* \end{aligned}$$

and

$$\begin{aligned} \alpha^*\beta^* &= [(a - bu) - b\gamma] \cdot [(c - du) - d\gamma] \\ &= (a - bu)(c - du) + bd\gamma^2 - [(a - bu)d + (c - du)b]\gamma \\ &= (ac - adu - bcu + bdu^2) + bd(-u\gamma - v) - (ad + bc - 2bdu)\gamma \\ &= (ac - adu - bcu + bdu^2 - bdv) - (ad + bc - bdu)\gamma \end{aligned}$$

which is the same as

$$\begin{aligned} (\alpha\beta)^* &= [(a + b\gamma)(c + d\gamma)]^* \\ &= [ac + bd\gamma^2 + (ad + bc)\gamma]^* \\ &= [ac + bd(-u\gamma - v) + (ad + bc)\gamma]^* \\ &= [(ac - bdv) + (ad + bc - bdu)\gamma]^* \\ &= [(ac - bdv) - (ad + bc - bdu)u] - (ad + bc - bdu)\gamma \\ &= (ac - adu - bcu + bdu^2 - bdv) - (ad + bc - bdu)\gamma. \end{aligned}$$

Remark: The hardest part of the theory is to prove that generalized conjugation maps **exist**. This subject is called "Galois theory".

(c,d): Just check that the hints work. I won't do it because I got too tired on part (b).

(e): Given a nonzero element $\alpha = a + b\gamma \neq 0$ we have seen that $N(\alpha) = \alpha\alpha^* \neq 0$, hence we can rationalize the denominator:

$$\begin{aligned}\frac{1}{\alpha} &= \frac{1}{\alpha}\frac{\alpha^*}{\alpha^*} \\ &= \frac{\alpha^*}{N(\alpha)} \\ &= \frac{(a-bu)-b\gamma}{a^2-abu+b^2v} \\ &= \left(\frac{a-bu}{a^2-abu+b^2v}\right) + \left(\frac{-b}{a^2-abu+b^2v}\right)\gamma.\end{aligned}$$

Actually, this is not a real proof. It's just a heuristic method that lets us discover the correct formula.

Remark: I apologize that this problem was so computational, but we needed the results of parts (a) and (b) to study constructible numbers in Problem 4. Parts (c,d,e) show that the high school trick of rationalizing the denominator is a lot deeper than it looks.

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.]

(a): Consider some integers $a, b, c \in \mathbb{Z}$ with $\gcd(a, b) = 1$. From the Extended Euclidean Algorithm we can find some integers $x, y \in \mathbb{Z}$ satisfying $ax + by = 1$. Multiply by c to get

$$\begin{aligned}ax + by &= 1 \\ (ax + by)c &= c \\ acx + bcy &= c.\end{aligned}$$

If $a|bc$ (say $ak = bc$) then it follows that

$$\begin{aligned}acx + (bc)y &= c \\ acx + (ak)y &= c \\ a(cx + ky) &= c,\end{aligned}$$

and hence $a|c$.

(b): Consider any polynomial $f(x) = c_n x^n + \cdots + c_1 x + c_0 \in \mathbb{Z}[x]$ and suppose that $f(a/b) = 0$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$ and $\gcd(a, b) = 1$. Multiplying both sides of the equation $f(a/b) = 0$ by b^n gives

$$\begin{aligned}c_n\left(\frac{a}{b}\right)^n + \cdots + c_1\left(\frac{a}{b}\right) + c_0 &= 0 \\ c_n\left(\frac{a}{b}\right)^n b^n + \cdots + c_1\left(\frac{a}{b}\right) b^n + c_0 b^n &= 0 \\ c_n a^n + c_{n-1}a^{n-1}b + \cdots + c_1 a b^{n-1} + c_0 b^n &= 0.\end{aligned}$$

Since $c_0 b^n = a(\text{some integer})$ and $\gcd(a, b) = 1$ it follows from (a) that $a|c_0$. Since $c_n a^n = b(\text{some integer})$ and $\gcd(a, b) = 1$ it follows from (a) that $b|c_n$.

Remark: For any integer polynomial $f(x) \in \mathbb{Z}[x]$ we can use this test to find all rational roots of $f(x)$, or prove that none exist. We will use this in Problem 6.

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 $\mathbb{F}_k$.]

(a): Consider a quadratic field extension $\mathbb{E} \supseteq \mathbb{F}$ with conjugation map $* : \mathbb{E} \to \mathbb{E}$ satisfying the following properties:[3]

- For all $\alpha \in \mathbb{E}$ we have $\alpha = \alpha^*$ if and only if $\mathbb{F}$.
- For all $\alpha, \beta \in \mathbb{E}$ we have $(\alpha + \beta)^* = \alpha^* + \beta^*$ and $(\alpha\beta)^* \alpha^* \beta^*$.
- For all $\alpha \in \mathbb{E}$ we have $\alpha + \alpha^* \in \mathbb{F}$ and $\alpha\alpha^* \in \mathbb{F}$.

For any polynomial $f(x) \in \mathbb{E}$ of degree 3 we will show that

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

So suppose that $f(\alpha) = 0$ for some $\alpha \in \mathbb{E}$. If $\alpha \in \mathbb{F}$ then we are done. Otherwise, we have $\alpha \neq \alpha^*$. But α^* is also a root of $f(x)$ because[4]

$$f(\alpha^*) = [f(\alpha)]^* = 0^* = 0.$$

Since $f(\alpha) = 0$, Descartes' Theorem gives $f(x) = (x - \alpha)g(x)$ for some $g(x) \in \mathbb{E}[x]$. Then substituting $x = \alpha^*$ gives

$$\begin{aligned} f(\alpha^*) &= (\alpha^* - \alpha)g(\alpha^*) \\ 0 &= (\alpha^* - \alpha)g(\alpha^*) \\ 0 &= g(\alpha^*), \end{aligned}$$

because $\alpha^* - \alpha \neq 0$. Applying Descartes' Theorem again gives $g(x) = (x - \alpha^*)h(x)$ for some $h(x) \in \mathbb{E}[x]$, so that

$$\begin{aligned} f(x) &= (x - \alpha)(x - \alpha^*)h(x) \\ f(x) &= (x^2 - (\alpha + \alpha^*)x + \alpha\alpha^*)h(x). \end{aligned}$$

Since $\alpha + \alpha^* \in \mathbb{F}$ and $\alpha\alpha^* \in \mathbb{F}$ it follows from Problem 2 on Homework 4 that $h(x) \in \mathbb{F}[x]$. Finally, since $\deg(f) = 3$ we must have $\deg(h) = 1$. Since any polynomial $h(x) \in \mathbb{F}[x]$ of

[3] We can write $\mathbb{E} = \mathbb{F}[\gamma]$ for some γ satisfying an irreducible quadratic equation over $\mathbb{F}$. Then the conjugation map $*$ has an explicit formula as in Problem 3. However, it is not necessary to mention γ in this problem.

[4] The proof that $[f(\alpha)]^* = f(\alpha^*)$ is the exactly the same as for complex conjugation. You proved this on Exam 2.

degree 1 has a root in $\mathbb{F}$, it follows that $f(x)$ has a root in $\mathbb{F}$. (To be explicit, we must have $h(x) = a + bx$ for some $a, b \in \mathbb{F}$ with $b \neq 0$. Then $h(-a/b) = 0$ and hence $f(-a/b) = 0$.)

(b): Consider a polynomial $f(x) \in \mathbb{Q}[x]$ of degree 3 and suppose that $f(x)$ has a constructible root $\alpha \in \mathbb{R}$. By definition this means that α is contained in a chain of quadratic field extensions:

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

We will use induction to show that $f(x)$ has a root in $\mathbb{Q}$. To be specific, we observe that the following implication holds for all $1 \leq k \leq n$:

$$f(x) \text{ has a root in } \mathbb{F}_k \quad \Longrightarrow \quad f(x) \text{ has a root in } \mathbb{F}_{k-1}.$$

Indeed, suppose that $f(x)$ has a root in $\mathbb{F}_k$. Since $f(x)$ has degree 3 and has coefficients in $\mathbb{F}_{k-1}$ (because $\mathbb{F}_{k-1}$ contains $\mathbb{Q}$) it follows from (a) that $f(x)$ has a root in $\mathbb{F}_{k-1}$.

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 $\theta = \pi/9$.]

(a): Let $f(x) = x^3 - 2 \in \mathbb{Z}[x]$. If $f(a/b) = 0$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$ and $\gcd(a, b) = 1$ then Problem 4b says that $a|2$ and $b|1$, so that $a/b = \pm 2$ or ± 1. But none of these four numbers is a root of $f(x)$, hence $f(x)$ has no rational root.

Remark: It follows from Problem 5b that the polynomial $f(x)$ has no constructible roots. Since $\sqrt[3]{2}$ is a root of $f(x)$ it follows that $\sqrt[3]{2}$ is not constructible. This shows that the classical "Delian problem" is impossible:

`https://en.wikipedia.org/wiki/Doubling_the_cube`

(b): Let $\omega = \exp(2\pi i/7)$ so that

$$\alpha = \omega + \omega^{-1} = [\cos(2\pi/7) + i\sin(2\pi/7)] + [\cos(2\pi/7) - i\sin(2\pi/7)] = 2\cos(2\pi/7).$$

We showed on a previous homework that

$$1 + \omega + \omega^2 + \omega^3 + \omega^4 + \omega^5 + \omega^6 = 0$$
$$1 + \omega + \omega^2 + \omega^3 + \omega^{-3} + \omega^{-2} + \omega^{-1} = 0.$$

On the other hand, we have

$$\alpha^3 = (\omega + \omega^{-1})^3 = \omega^3 + 3\omega^1 + 3\omega^{-1} + \omega^{-3},$$
$$\alpha^2 = (\omega + \omega^{-1})^2 = \omega^2 + 2 + \omega^{-2},$$

$$\alpha = \omega^1 + \omega^{-1},$$

so that

$$\alpha^3 + \alpha^2 - 2\alpha - 1 = 1 + \omega + \omega^2 + \omega^3 + \omega^{-3} + \omega^{-2} + \omega^{-1} = 0.$$

We have shown that the real number $2\cos(2\pi/7) \in \mathbb{R}$ is a root of the integer polynomial $f(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Z}[x]$. According to the rational root test, if $f(a/b) = 0$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$ and $\gcd(a, b) = 1$ then we must have $a|1$ and $b|1$ so that $a/b = \pm 1$. But ± 1 are not roots of $f(x)$, hence $f(x)$ has no rational root.

Remark: It follows from Problem 5b that the polynomial $f(x)$ has no constructible roots. Since $2\cos(2\pi/7)$ is a root of $f(x)$ it follows that $2\cos(2\pi/7)$ is not constructible. This shows that the regular heptagon is not constructible with ruler and compass. For more:

`https://en.wikipedia.org/wiki/Heptagon`

(c): To show that $\alpha = 2\cos(\pi/9)$ is a root of $x^3 - 2x - 1$ we will use de Moivre's theorem. To save space we will write $c = \cos\theta$ and $s = \sin\theta$:

$$\begin{aligned}
\cos(3\theta) + i\sin(3\theta) &= (c + is)^3 \\
&= (c + is)(c + is)^2 \\
&= (c + is)[(c^2 - s^2) + (2cs)i] \\
&= [c(c^2 - s^2) - 2cs^2] + [2c^2 s + s(c^2 - s^2)]i
\end{aligned}$$

Comparing real parts gives[5]

$$\begin{aligned}
\cos(3\theta) &= c(c^2 - s^2) - 2cs^2 \\
&= c^3 - cs^2 - 2cs^2 \\
&= c^3 - 3cs^2 \\
&= c^3 - 3c(1 - c^2) && \text{because } c^2 + s^2 = 1 \\
&= c^3 - 3c + 3c^4 \\
&= 4c^3 - 3c \\
&= 4\cos^3\theta - 3\cos\theta.
\end{aligned}$$

Now substitute $\theta = \pi/9$ to get

$$\begin{aligned}
4\cos^3(\pi/9) - 3\cos(\pi/9) &= \cos(\pi/3) \\
4\cos^3(\pi/9) - 3\cos(\pi/9) &= 1/2 \\
4(\alpha/2)^3 - 3(\alpha/2) &= 1/2 \\
4\alpha^3/8 - 3\alpha/2 &= 1/2 \\
\alpha^3 - 3\alpha &= 1 \\
\alpha^3 - 3\alpha - 1 &= 0.
\end{aligned}$$

If the polynomial $f(x) = x^3 - 3x - 1 \in \mathbb{Z}[x]$ satisfies $f(a/b) = 0$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$ and $\gcd(a, b) = 1$ then the rational root test says that $a|1$ and $b|1$, hence $a/b = \pm 1$. But ± 1 are not roots of $f(x)$, hence $f(x)$ has no rational root.

[5]Comparing imaginary parts gives $\sin(3\theta) = 3\sin\theta - 4\sin^3\theta$, but we don't need this.

Remark: It follows from Problem 5b that the polynomial $f(x)$ has no constructible roots. Since $2\cos(\pi/9)$ is a root of $f(x)$ it follows that $2\cos(\pi/9)$ is not constructible. This shows that it is impossible to trisect an arbitrary angle using ruler and compass. Indeed, the angle $\pi/3$ is constructible. If it were possible to trisect any angle then $\pi/9$ would be constructible. For more:

`https://en.wikipedia.org/wiki/Angle_trisection`