Math 461 **Spring 2020**
Homework 2 **Drew Armstrong**

Problem 1. One Real Root. Consider a polynomial $x^3 + px + q$ with real coefficients $p, q \in \mathbb{R}$ satisfying $p > 0$. We will show that this polynomial has exactly one real root.

(a) From the Intermediate Value Theorem we know that there exists a real root $f(r) = 0$. In this case use long division to show that

$$f(x) = (x - r)(x^2 + rx + p + r^2).$$

(b) Show that $x^2 + rx + p + r^2$ has no real roots. [Hint: Consider the discriminant.]

(a): Applying the long division algorithm gives

$$\begin{array}{r|llll}
 & x^2 & +rx & +(p+r^2) & \\ \hline
x - r & x^3 & & +px & +q \\
 & x^3 & -rx^2 & & \\ \hline
 & & rx^2 & +px & +q \\
 & & rx^2 & -r^2x & \\ \hline
 & & & (p+r^2)x & +q \\
 & & & (p+r^2)x & -(p+r^2)r \\ \hline
 & & & & q+(p+r^2)r
\end{array}$$

And we observe that the remainder is zero: $r(r^2 + p) + q = r^3 + rp + q = f(r) = 0$.

(b): For any real number $s \in \mathbb{R}$ satisfying $f(s) = 0$ and $s \neq r$ we have

$$(s - r)(s^2 + rs + p + r^2) = f(s) = 0,$$

which implies that $s^2 + rs + p + r^2 = 0$, hence s is a real root of $x^2 + rx + p + r^2 = 0$. However, since $p > 0$ we observe that this quadratic equation has no real roots because it has a negative discriminant:

$$r^2 - 4(p + r^2) = -3r^2 - 4p < 0.$$

Problem 2. Coefficients Versus Roots. Let $\mathbb{F}$ be a field and suppose that the polynomial $f(x) = x^3 + ax^2 + bx + c \in \mathbb{F}[x]$ has three roots $r, s, t \in \mathbb{F}$.

(a) Find formulas for a, b, c in terms of r, s, t.

(b) Find a formula for $r^2 + s^2 + t^2$ in terms of a, b, c. [Hint: Square $r + s + t$.]

(a): If $r, s, t \in \mathbb{F}$ are distinct roots of $x^3 + ax^2 + bx + c \in \mathbb{F}[x]$ then we may use Descartes' Factor Theorem to obtain

$$\begin{aligned}
x^3 + ax^2 + bx + c &= (x - r)(x - s)(x - t) \\
&= x^3 - (r + s + t)x^2 + (rs + rt + st)x - rst.
\end{aligned}$$

Then comparing coefficients gives

$$\left\{\begin{array}{lcl}
a &=& -(r + s + t), \\
b &=& rs + rt + st, \\
c &=& -rst.
\end{array}\right.$$

(b): It follows that

$$\begin{aligned}
(r+s+t)^2 &= r^2+s^2+t^2+2rs+2rt+2st \\
(-a)^2 &= r^2+s^2+t^2+2(rs+rt+st) \\
a^2 &= r^2+s^2+t^2+2b \\
a^2-2b &= r^2+s^2+t^2.
\end{aligned}$$

Problem 3. Uniqueness of Roots. Let $f(x) \in \mathbb{F}[x]$ be a polynomial with coefficients in a field $\mathbb{F}$. Suppose that there exist numbers $a_1, \ldots, a_r \in \mathbb{F}$ and $b_1, \ldots, b_s \in \mathbb{F}$ such that

$$f(x) = (x-a_1)(x-a_2)\cdots(x-a_r) = (x-b_1)(x-b_2)\cdots(x-b_s).$$

(a) Prove that $r = s$. [Hint: Degree.]
(b) Prove that the roots can be re-indexed so that $a_i = b_i$ for all i. [Hint: Consider $f(a_1)$.]

(a): Comparing degrees gives

$$\begin{aligned}
(x-a_1)(x-a_2)\cdots(x-a_r) &= (x-b_1)(x-b_2)\cdots(x-b_s) \\
\deg\left((x-a_1)(x-a_2)\cdots(x-a_r)\right) &= \deg\left((x-b_1)(x-b_2)\cdots(x-b_s)\right) \\
\deg(x-a_1)+\cdots+\deg(x-a_r) &= \deg(x-b_1)+\cdots+\deg(x-b_s) \\
\underbrace{1+\cdots+1}_{r\text{ times}} &= \underbrace{1+\cdots+1}_{s\text{ times}} \\
r &= s.
\end{aligned}$$

(b): Substituting $x = a_1$ gives

$$\begin{aligned}
(a_1-a_1)(a_1-a_2)\cdots(a_1-a_r) &= (a_1-b_1)(a_1-b_2)\cdots(a_1-b_s) \\
0\cdot(a_1-a_2)\cdots(a_1-a_r) &= (a_1-b_1)(a_1-b_2)\cdots(a_1-b_s) \\
0 &= (a_1-b_1)(a_1-b_2)\cdots(a_1-b_s).
\end{aligned}$$

It follows that $a_1 - b_i = 0$ for some i, and after re-indexing we may assume that $a_1 = b_1$. Now we may cancel the factor $x - a_1$ from both sides to obtain

$$\begin{aligned}
\cancel{(x-a_1)}(x-a_2)\cdots(x-a_r) &= \cancel{(x-a_1)}(x-b_2)\cdots(x-b_s) \\
(x-a_2)\cdots(x-a_r) &= (x-b_2)\cdots(x-b_s),
\end{aligned}$$

and the result follows by induction.

Problem 4. Cardano's Formula. Cardano's formula applied to $x^3+6x-20=0$ gives

$$x = \sqrt[3]{10+\sqrt{108}} + \sqrt[3]{10-\sqrt{108}}.$$

Observe that $\sqrt{108} = 6\sqrt{3}$. Try to find some integers $a, b, c, d \in \mathbb{Z}$ such that

$$(a+b\sqrt{3})^3 = 10+\sqrt{108} \quad \text{and} \quad (c+d\sqrt{3})^3 = 10-\sqrt{108}.$$

Then use your answer to prove that

$$\sqrt[3]{10+\sqrt{108}} + \sqrt[3]{10-\sqrt{108}} = 2.$$

First we observe that

$$\begin{aligned}(a+b\sqrt{3})^3 &= a^3 + 3a^2(b\sqrt{3}) + 3a(b\sqrt{3})^2 + (b\sqrt{3})^3 \\ &= a^3 + 3a^2b\sqrt{3} + 9ab^2 + 3b^3\sqrt{3} \\ &= (a^3 + 9ab^2) + (3a^2b + 3b^3)\sqrt{3} \\ &= a(a^2+9b^2) + 3b(a^2+b^2)\sqrt{3}.\end{aligned}$$

We would like to find integers $a, b \in \mathbb{Z}$ such that $a(a^2+9b^2) = 10$ and $3b(a^2+b^2) = 6$. After a bit of trial and error, we see that the only solution is $a = 1$ and $b = 1$. In other words, the unique real cube root of $10 + \sqrt{108} = 10 + 6\sqrt{3}$ is equal to $1 + \sqrt{3}$. A similar argument shows that $1 - \sqrt{3}$ is the unique real cube root of $10 - \sqrt{108}$. Thus we conclude that

$$\sqrt[3]{10+\sqrt{108}} + \sqrt[3]{10-\sqrt{108}} = (1+\sqrt{3}) + (1-\sqrt{3}) = 2.$$

Problem 5. A Prime Cubic Polynomial. We will give a rigorous proof that the polynomial $f(x) = x^3 + x + 1$ is a prime element of the ring $\mathbb{Q}[x]$.

(a) Suppose that we have $f(a/b) = 0$ for some integers $a, b \in \mathbb{Z}$. By reducing a/b to lowest terms we may assume that a and b have no common prime factors. In this case show that $a = \pm 1$ and $b = \pm 1$. [Hint: If $p|a$ for some prime $p \in \mathbb{Z}$, then $p|b^3$ and hence $p|b$.]

(b) Use part (a) to show that $f(x)$ has no roots in $\mathbb{Q}$.

(c) Show that every polynomial in $\mathbb{Q}[x]$ of degree 1 has a root in $\mathbb{Q}$.

(d) If $f(x) \in \mathbb{Q}[x]$ is **not** prime then we can write $f(x) = g(x)h(x)$ for some polynomials $g(x), h(x) \in \mathbb{Q}[x]$ with $\deg(g) > 0$ and $\deg(h) > 0$. Show that one of $g(x)$ or $h(x)$ must have degree 1 and use this to obtain a contradiction.

(a): Substituting $x = a/b$ and clearing denominators gives

$$\begin{aligned} f(a/b) &= 0 \\ (a/b)^3 + (a/b) + 1 &= 0 \\ a^3/b^3 + a/b + 1 &= 0 \\ a^3 + ab^2 + b^3 &= 0. \end{aligned}$$

Suppose that a has a prime factor $p|a$. Since $b^3 = a(-a^2 - b^2)$ we conclude that $p|b^3$ and then from Euclid's Lemma we obtain $p|b$. But this contradicts the fact that a and b have no common prime factors. Therefore a has no prime factor; in other words, we must have $a = \pm 1$. Similarly, if b has a prime factor $q|b$ then we observe that $q|a^3$ and hence $q|a$. This contradiction shows that b had no prime factors and hence $b = \pm 1$.

(b): If $a/b \in \mathbb{Q}$ is a rational root of $f(x)$ (in lowest terms) then from part (a) we know that $a = \pm 1$ and $b = \pm 1$, hence $a/b = \pm 1$. But we observe that $f(1) = 3 \neq 0$ and $f(-1) = -1 \neq 0$. Therefore $f(x)$ has no rational root.

(c): Let $g(x) \in \mathbb{Q}[x]$ have degree 1, say $g(x) = (a/b)x + (c/d)$ for some $a, b, c, d \in \mathbb{Z}$. Then we observe that

$$g\left(\frac{-bc}{ad}\right) = \frac{a}{b}\left(-\frac{bc}{ad}\right) + \frac{c}{d} = -\frac{c}{d} + \frac{c}{d} = 0.$$

Hence $g(x)$ has the rational root $-(bc)/(ad) \in \mathbb{Q}$.

(d): Assume for contradiction that $f(x) = x^3 + x + 1 \in \mathbb{Q}[x]$ is **not** prime in $\mathbb{Q}[x]$. By definition this means we can write $f(x) = g(x)h(x)$ for some polynomials $g(x), h(x) \in \mathbb{Q}[x]$ with $\deg(g) \geq 1$ and $\deg(h) \geq 1$. Comparing degrees gives

$$\begin{aligned} f(x) &= g(x)h(x) \\ \deg(f) &= \deg(gh) \\ 3 &= \deg(g) + \deg(h), \end{aligned}$$

therefore we must have $\deg(g) = 1$ and $\deg(h) = 2$ or $\deg(g) = 2$ and $\deg(h) = 1$. Without loss of generality let us assume that $\deg(g) = 1$. Then from part (c) there exists rational number $\alpha \in \mathbb{Q}$ satiasfying $g(\alpha) = 0$. Finally, by substituting $x = \alpha$ we obtain

$$f(\alpha) = g(\alpha)h(\alpha) = 0 \cdot h(\alpha) = 0,$$

which contradicts the fact that $f(x)$ has no rational root. $\square$

Discussion: Part (a) was the trickiest problem on this homework assignment. We can generalize this argument as follows. Consider any polynomial $f(x) = c_0 + c_1 x + \cdots + c_n x^n \in \mathbb{Z}[x]$ with integer coefficients and suppose that we have $f(a/b) = 0$ for some fraction $a/b \in \mathbb{Q}$ written in lowest terms. By substituting and clearing denominators we obtain the following equation of integers:

$$c_0 b^n + c_1 a b^{n-1} + \cdots + c_{n-1} a^{n-1} b + c_n a^n = 0.$$

It follows from this that $a|c_0 b^n$ and $b|c_n a^n$. Finally, since a and b have no common factors, one can show using Euclid's Lemma (proof omitted) that we must have $a|c_0$ and $b|c_n$. This argument is called the *rational root test*. It restricts the possible rational roots of $f(x)$ to a finite set, which can be checked by hand.

Problem 6. Complex Conjugation. Let i be an abstract symbol satisfying $i^2 = -1$ and consider the ring of complex numbers:

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}.$$

We define *complex conjugation* $* : \mathbb{C} \to \mathbb{C}$ by the following formula:

$$(a + bi)^* := a - bi.$$

(a) For all $\alpha \in \mathbb{C}$ show $\alpha^* = \alpha$ if and only if $\alpha \in \mathbb{R}$.
(b) For all $\alpha, \beta \in \mathbb{C}$ show that $(\alpha + \beta)^* = \alpha^* + \beta^*$ and $(\alpha\beta)^* = \alpha^* \beta^*$.
(c) For all real polynomials $f(x) \in \mathbb{R}[x]$ and complex numbers $\alpha \in \mathbb{C}$ show that

$$f(\alpha)^* = f(\alpha^*).$$

(d) Use part (c) to show that complex roots of real polynomials come in conjugate pairs. It follows that any real polynomial has an **even number** of complex roots.

Before we begin, let me make three important observations:

- The abstract symbol i (whatever it is) is not a real number. If it were, then from trichotomy we would have $i < 0$ or $i = 0$ or $i > 0$. But $i < 0$ implies $0 < i^2 = -1$, $0 = i$ implies $0 = i^2 = -1$, and $0 < i$ implies $0 < i^2 = -1$, all of which are false.
- For all real numbers $a, b, c, d \in \mathbb{R}$ I claim that

$$a + bi = c + di \quad \Leftrightarrow \quad a = c \text{ and } b = d.$$

Indeed, if $a = c$ and $b = d$ then $a + bi = c + di$. Conversely, suppose that $a + bi = c + di$. If $b \neq d$ then we conclude that $i = (a - c)/(d - b)$ is real, which contradicts the previous remark. Therefore we must have $b = d$ and hence $a = c$.

- We view $\mathbb{R}$ as a subset of $\mathbb{C}$ by identifying the real number $a \in \mathbb{R}$ with the complex number $a + 0i \in \mathbb{C}$. It follows that $a + bi \in \mathbb{R}$ if and only if $b = 0$.

(a): Consider any $\alpha = a + bi \in \mathbb{C}$. If α is real then $b = 0$ and hence

$$\alpha^* = (a + 0i)^* = a - 0i = a + 0i = \alpha.$$

Conversely, suppose that $\alpha^* = \alpha$, so that $a + bi = a - bi$. Subtracting a on both sides gives $bi = -bi$, which implies that $2bi = 0$ and hence $b = 0$.[1] It follows that $\alpha = a + 0i$ is real.

(b): Let $\alpha = a + bi$ and $\beta = c + di$. Then we have

$$\begin{aligned}\alpha^* + \beta^* &= (a - bi) + (c - di)\\ &= (a + c) - (b + d)i\\ &= ((a + c) + (b + d)i)^*\\ &= (\alpha + \beta)^*\end{aligned}$$

and

$$\begin{aligned}\alpha^*\beta^* &= (a - bi)(c - di)\\ &= ac - adi - bci + bdi^2\\ &= ac - adi - bci - bd\\ &= (ac - bd) - (ad + bc)i\\ &= ((ac - bd) + (ad + bc)i)^*\\ &= ((a + bi)(c + di))^*\\ &= (\alpha\beta)^*.\end{aligned}$$

(c): Consider any polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{R}[x]$ with real coefficients and let $\alpha \in \mathbb{C}$ be any complex number. Then combining parts (a) and (b) gives

$$\begin{aligned}f(\alpha)^* &= (a_0 + a_1\alpha + \cdots + a_n\alpha^n)^*\\ &= a_0^* + a_1^*\alpha^* + \cdots + a_n^*(\alpha^*)^n && \text{(b)}\\ &= a_0 + a_1\alpha^* + \cdots + a_n(\alpha^*)^n && \text{(a)}\\ &= f(\alpha^*).\end{aligned}$$

(d): We conclude from part (c) that

$$f(\alpha) = 0 \quad \Leftrightarrow \quad f(\alpha)^* = 0 \quad \Leftrightarrow \quad f(\alpha^*) = 0.$$

In other words, $\alpha \in \mathbb{C}$ is a root of $f(x) \in \mathbb{R}[x]$ if and only if $\alpha^* \in \mathbb{C}$ is a root of $f(x)$. This tells us that the non-real complex roots of $f(x)$ come in pairs. Hence there must be an even number of non-real complex roots (possibly zero).

Discussion: This problem was intended to get you thinking about complex numbers. In the next chapter I will give a thorough treatement, after which this problem will make a lot more sense.

[1] From the above remarks, if $0 + 2bi = 0 + 0i$ then $2b = 0$, which then implies that $b = 0$.