Math 461 Spring 2020
Homework 4 Drew Armstrong

Problem 1. Complex Numbers as Real 2×2 Matrices. For any complex number $\alpha = a + bi \in \mathbb{C}$ with $a, b \in \mathbb{R}$ we define the following matrix:

$$M_\alpha := \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

(a) Check that for all $r \in \mathbb{R}$ and $\alpha \in \mathbb{C}$ we have $M_{(r\alpha)} = rM_\alpha$.
(b) Check that for all $\alpha, \beta \in \mathbb{C}$ we have $M_{\alpha+\beta} = M_\alpha + M_\beta$ and $M_{\alpha\beta} = M_\alpha M_\beta$.
(c) Check that for all $\alpha \in \mathbb{C}$ we have $\det(M_\alpha) = |\alpha|^2$.
(d) Check that for all $\alpha \in \mathbb{C}$ we have $(M_\alpha)^* = M_{(\alpha^*)}$, where the star operation denotes the transpose matrix and the complex conjugate, respectively.

(a): For all $r \in \mathbb{R}$ and $\alpha = a + bi \in \mathbb{C}$ we have

$$M_{(r\alpha)} = M_{(ra+rbi)} = \begin{pmatrix} ra & -rb \\ rb & ra \end{pmatrix} = r \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = rM_\alpha.$$

(b): For all $\alpha = a + bi \in \mathbb{C}$ and $\beta = c + di \in \mathbb{C}$ we have

$$M_{\alpha+\beta} = M_{(a+c)+(b+d)i} = \begin{pmatrix} a+c & -(b+d) \\ b+d & a+c \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = M_\alpha + M_\beta.$$

Furthermore, since $\alpha\beta = (ac - bd) + (ad + bc)i$, we have

$$\begin{aligned} M_\alpha M_\beta &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \\ &= \begin{pmatrix} ac - bd & -ad - bc \\ bc + ad & -bd + ac \end{pmatrix} \\ &= \begin{pmatrix} ac - bd & -(ad + bc) \\ ad + bc & ac - bd \end{pmatrix} = M_{\alpha\beta}. \end{aligned}$$

(c): For all $\alpha = a + bi \in \mathbb{C}$ we have

$$\det(M_\alpha) = \det \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = aa - (-b)b = a^2 + b^2 = |\alpha|^2.$$

[Remark: For all $\alpha, \beta \in \mathbb{C}$, it follows from the multiplicative property of determinants that

$$|\alpha|^2|\beta|^2 = \det(M_\alpha)\det(M_\beta) = \det(M_\alpha M_\beta) = \det(M_{\alpha\beta}) = |\alpha\beta|^2.$$

This is another way to prove the multiplicative property of absolute value.]

[Remark: There wasn't really anything to do in this problem. I just wanted you to observe that these facts are true. In modern jargon, we say that the function $\alpha \mapsto M_\alpha$ is an **injective homomorphism of $\mathbb{R}$-algebras.**]

(d): For all $\alpha = a + bi \in \mathbb{C}$ we have

$$(M_\alpha)^* = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}^* = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} a & -(-b) \\ -b & a \end{pmatrix} = M_{a-bi} = M_{(\alpha^*)}.$$

Problem 2. Greatest Common Divisor. Let $a, b \in \mathbb{Z}$ with $d = \gcd(a,b)$. Since d is a common divisor of a and b we must have $a = da'$ and $b = db'$ for some integers $a', b' \in \mathbb{Z}$. In this case, prove that the numbers a', b' are *coprime*:

$$\gcd(a', b') = 1.$$

[HInt: From Bézout's Identity we know that $ax + by = d$ for some (non-unique) integers $x, y \in \mathbb{Z}$. Use this to show that any common divisor $e|a'$ and $e|b'$ must satisfy $e|1$.]

Proof. Let $d = \gcd(a,b)$ with $a = da'$ and $b = db'$ for some integers $a', b' \in \mathbb{Z}$. From Bézout's Identity there exist some $x, y \in \mathbb{Z}$ such that $ax + by = d$, hence we have

$$\begin{aligned} ax + by &= d \\ da'x + db'y &= d \\ \not{d}(a'x + b'y) &= \not{d} \\ a'x + b'y &= 1. \end{aligned}$$

We will use this equation to show that $\gcd(a', b') = 1$. To do this, let e be any common divisor of a' and b', so that $a' = ea''$ and $b' = db''$ for some integers $a'', b'' \in \mathbb{Z}$. It follows that

$$\begin{aligned} a'x + b'y &= 1 \\ ea''x + eb''y &= 1 \\ e(a''x + b''y) &= 1. \end{aligned}$$

But this implies that $e = \pm 1$, hence the greatest common divisor of a'' and b'' is 1. $\square$

Problem 3. Euclid's Lemma. For all integers $a, b, c \in \mathbb{Z}$, prove that

$$(a|bc \text{ and } \gcd(a,b) = 1) \quad \Rightarrow \quad a|c.$$

[Hint: If $\gcd(a,b) = 1$ then from Bézout's Identity there exist some (non-unique) integers $x, y \in \mathbb{Z}$ satisfying $ax + by = 1$. Multiply both sides by c to get $acx + bcy = c$. Now what?]

Proof. Suppose that $a|bc$; say $ak = bc$ for some $k \in \mathbb{Z}$. Suppose also that $\gcd(a,b) = 1$, hence from Bézout's Identity we have $ax + by = 1$ for some $x, y \in \mathbb{Z}$. Not multiply both sides by c to obtain

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

We conclude that $a|c$, as desired. $\square$

Problem 4. Rational Root Test. Let $f(x) = c_n x^n + \cdots + c_1 x + c_0 \in \mathbb{Z}[x]$ be a polynomial of degree n with integer coefficients. Suppose that $f(x)$ has a rational root $a/b \in \mathbb{Q}$ in lowest terms, i.e., with $\gcd(a,b) = 1$. In this case, prove that we must have

$$a|c_0 \quad \text{and} \quad b|c_n.$$

[HInt: Suppose that $f(a/b) = 0$. Multiply both sides by b^n and then use Euclid's Lemma.]

Proof. Let $f(a/b) = 0$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$ and $\gcd(a, b) = 1$. Then we have

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

By taking the term $c_0 b^n$ to one side, we have

$$\begin{aligned} c_0 b^n &= -c_n a^n - c_{n-1}a^{n-1}b - \cdots - c_1 ab^{n-1} \\ &= a\left[-c_n a^{n-1} - c_{n-1}a^{n-2}b - \cdots - c_1 b^{n-1}\right]. \end{aligned}$$

which implies that $a|c_0 b^n$. Then since $\gcd(a, b) = 1$, Euclid's Lemma implies that $a|c_0$. Similarly, by taking the term $c_n a^n$ to one side, we have

$$\begin{aligned} c_n a^n &= -c_{n-1}a^{n-1}b - \cdots - c_1 ab^{n-1} - c_0 b^n \\ &= b\left[-c_{n-1}a^{n-1} - \cdots - c_1 ab^{n-2} - c_0 b^{n-1}\right], \end{aligned}$$

hence $b|c_n a^n$. Then since $\gcd(a, b) = 1$, Euclid's Lemma implies that $b|c_n$. □

Example. This result gives an algorithm to quickly find all of the rational roots of any polynomial with integer coefficients. For example, let $f(x) = 4x^3 - 12x^2 + 11x - 3$. If $f(a/b) = 0$ for some fraction $a/b \in \mathbb{Q}$ in lowest terms, then the Rational Root Test says that $a|3$ and $b|4$, which leads to a finite list of potential rational roots:

$$\frac{a}{b} \in \left\{\pm 1, \pm 3, \pm\frac{1}{2}, \pm\frac{3}{2}, \pm\frac{1}{4}, \pm\frac{3}{4}\right\}.$$

By direct checking we find that 1, 1/2 and 3/2 are actual roots, hence

$$f(x) = 4(x-1)(x-1/2)(x-3/2).$$

This method does **not** help us to find non-rational roots.

Problem 5. The Regular 7-Gon. Let $\omega = e^{2\pi i/7}$ and $\alpha = \omega + \omega^{-1} = 2\cos(2\pi/7)$.

(a) Combine the numbers $1, \alpha, \alpha^2, \alpha^3$ to find some polynomial $f(x) \in \mathbb{Z}[x]$ of degree 3 satisfying $f(\alpha) = 0$. [Hint: Use the fact that $\omega^3 + \omega^2 + \omega + 1 + \omega^{-1} + \omega^{-2} + \omega^{-3} = 0$.]
(b) Use Problem 4 to show that your polynomial $f(x)$ from part (a) has no rational roots.
(c) Use part (b) to prove that the real number $\cos(2\pi/7) \in \mathbb{R}$ is **irrational**.

(a): First we compute the powers of α:

$$\begin{array}{ccccccccccccccc} 1 & = & & & & & & & 1 & & & & & & \\ \alpha & = & & & & & \omega & + & 0 & + & \omega^{-1} & & & & \\ \alpha^2 & = & & & \omega^2 & + & 0 & + & 2 & + & 0 & + & \omega^2 & & \\ \alpha^3 & = & \omega^3 & + & 0 & + & 3\omega & + & 0 & + & 3\omega^{-1} & + & 0 & + & \omega^{-3} \end{array}$$

Working from outside in, we find that

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

Therefore we define $f(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Z}[x]$ and we observe that $f(\alpha) = 0$.

(b): Suppose that $f(x)$ has a rational root, so that $f(a/b) = 0$ for some integers $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$. Then from part (b) we must have $a|1$ and $b|1$, hence $a/b = \pm 1$. But we observe that $f(1) - 1 \neq 0$ and $f(-1) = -3 \neq 0$. Hence the polynomial $f(x)$ has no rational roots, and it follows from part (a) that $\alpha = 2\cos(2\pi/7)$ is not rational.

(c): Assume for contradiction that $\cos(2\pi/7) = c/d$ for some integers $c, d \in \mathbb{Z}$. It follows that

$$\alpha = 2\cos\left(\frac{2\pi}{7}\right) = \frac{2c}{d} \in \mathbb{Q},$$

which contradicts part (b). Hence we conclude that $\cos(2\pi/7)$ is irrational. $\square$

[Remark: We will use this result later to prove that a regular 7-gon is not constructible with straightedge and compass.]

Problem 6. Conjugation of Complex Polynomials. For any polynomial $f(x) = \sum_{k\geq 0} a_k x^k \in \mathbb{C}[x]$ with complex coefficients, we define the *conjugate polynomial* as follows:

$$f^*(x) := \sum_{k\geq 0} a_k^* x^k.$$

(a) We can think of $\mathbb{R}[x] \subseteq \mathbb{C}[x]$ as a subring. For all $f(x) \in \mathbb{C}[x]$, prove that

$$f(x) \in \mathbb{R}[x] \quad \Leftrightarrow \quad f^*(x) = f(x).$$

(b) For all $f(x), g(x) \in \mathbb{C}[x]$, prove $(f+g)^*(x) = f^*(x) + g^*(x)$ and $(fg)^*(x) = f^*(x)g^*(x)$.
(c) For all $f(x) \in \mathbb{C}[x]$ use (a),(b) to prove that $f(x) + f^*(x) \in \mathbb{R}[x]$ and $f(x)f^*(x) \in \mathbb{R}[x]$.

(a): Recall that for all $a \in \mathbb{C}$ we have $a^* = a$ if and only if $a \in \mathbb{R}$. Then for all polynomials $f(x) = \sum_{k\geq 0} a_k x^k \in \mathbb{C}[x]$ we have

$$\begin{aligned} f^*(x) = f(x) &\Leftrightarrow \sum_{k\geq 0} a_k^* x^k = \sum_{k\geq 0} a_k x^k \\ &\Leftrightarrow a_k^* = a_k \text{ for all } k \geq 0 \\ &\Leftrightarrow a_k \in \mathbb{R} \text{ for all } k \geq 0 \\ &\Leftrightarrow f(x) \in \mathbb{R}[x]. \end{aligned}$$

(b): Recall that for all $a, b \in \mathbb{C}$ we have $(a+b)^* = a^* + b^*$ and $(ab)^* = a^* b^*$. Then for all $f(x) = \sum_{k\geq 0} a_k x^k \in \mathbb{C}[x]$ and $g(x) = \sum_{k\geq 0} b_k x^k \in \mathbb{C}[x]$ we have

$$\begin{aligned} (f+g)^*(x) &= \sum_{k\geq 0} (a_k + b_k)^* x^k \\ &= \sum_{k\geq 0} (a_k^* + b_k^*) x^k \\ &= \sum_{k\geq 0} a_k^* x^k + \sum_{k\geq 0} b_k^* x^k \\ &= f^*(x) + g^*(x) \end{aligned}$$

and

$$
\begin{aligned}
(fg)^*(x) &= \sum_{k\geq 0} \left(\sum_{i=1}^{k} a_i b_{k-i} \right)^* x^k \\
&= \sum_{k\geq 0} \left(\sum_{i=1}^{k} a_i^* b_{k-i}^* \right) x^k \\
&= \left(\sum_{k\geq 0} a_k^* x^k \right) \left(\sum_{k\geq 0} b_k^* x^k \right) \\
&= f^*(x) g^*(x).
\end{aligned}
$$

(c): For all $f(x) \in \mathbb{C}[x]$ we observe from part (b) that

$$(f + f^*)^*(x) = (f^* + f^{**})(x) = (f^* + f)(x) = (f + f^*)(x)$$

and

$$(ff^*)^*(x) = (f^* f^{**})(x) = (f^* f)(x) = (ff^*)(x).$$

Hence it follows from part (a) that $f(x) + f^*(x) \in \mathbb{R}[x]$ and $f(x)f^*(x) \in \mathbb{R}[x]$.

[Remark: We will use this last fact in our discussion of the Fundamental Theorem of Algebra. Here is a preview: Suppose that every real polynomial factors as a product of real polynomials of degrees 1 and 2. Now consider any complex polynomial $f(x) \in \mathbb{C}[x]$. Since $g(x) = f(x)f^*(x)$ has real coefficients we know that $g(x)$ factors as a product of real polynomials of degrees 1 and 2, hence by the quadratic formula we know that $g(x)$ splits over $\mathbb{C}$. Now suppose for contradiction that there exists a prime polynomial $p(x) \in \mathbb{C}[x]$ of degree ≥ 2 such that $p(x)|f(x)$. Then we also have $p(x)|g(x)$, which contradicts the fact that $g(x)$ splits over $\mathbb{C}$. We conclude that $f(x)$ also splits over $\mathbb{C}$. In summary, we have shown that the real version of the FTA implies the complex version of the FTA.]