Math 561/661 **Exam 1**
Fall 2021 **Fri Oct 1**

No electronic devices are allowed. There are 4 pages and each page is worth 6 points, for a total of 24 points.

Problem 1. Polar Form of Complex Numbers.

(a) State Euler's formula.

$$e^{i\theta} = \cos\theta + i\sin\theta$$

(b) Express -1 in polar form.

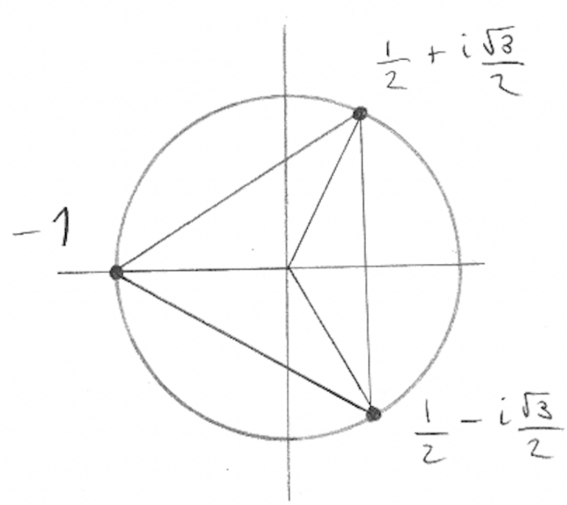
$$-1 = e^{i\pi}$$

(c) Find all of the 3rd roots of -1.

The primitive 3rd root of -1 is $e^{i\pi/3}$ and the 3rd roots of 1 are 1, $e^{2\pi i/3}$ and $e^{4\pi i/3}$. Therefore the 3rd roots of -1 are

$$\begin{aligned} e^{i\pi/3} &= \cos(\pi/3) + i\sin(\pi/3) = 1/2 + i\sqrt{3}/2, \\ e^{i\pi/3}e^{2\pi i/3} &= e^{i\pi} = \cos(\pi) + i\sin(\pi) = -1, \\ e^{i\pi/3}e^{4\pi/3} &= e^{i5\pi/3} = \cos(5\pi/3) + i\sin(5\pi/3) = 1/2 - i\sqrt{3}/2. \end{aligned}$$

Here is a picture:



(d) Use your answer from (c) to completely factor the polynomial $x^3 + 1$ over $\mathbb{C}$.

$$x^3 + 1 = (x - (-1))\left(x - (1/2 + i\sqrt{3}/2)\right)\left(x - (1/2 - i\sqrt{3}/2)\right)$$

Problem 2. Descartes' Factor Theorem. For any polynomials $f(x), g(x) \in \mathbb{F}[x]$ over a field $\mathbb{F}$ with $g(x) \neq 0$ there exist polynomials $q(x), r(x) \in \mathbb{F}[x]$ satisfying

$$\begin{cases} f(x) = g(x)q(x) + r(x), \\ \deg(r) < \deg(g). \end{cases}$$

You do not need to prove this.

(a) If $f(x) \in \mathbb{F}[x]$ satisfies $f(a) = 0$ for some $a \in \mathbb{F}$, prove that $f(x) = (x-a)q(x)$ for some polynomial $q(x) \in \mathbb{F}[x]$. [Hint: Divide $f(x)$ by $x - a$.]

There exist $q(x), r(x) \in \mathbb{F}[x]$ such that

$$\begin{cases} f(x) = (x-a)q(x) + r(x), \\ \deg(r) < \deg(x-a). \end{cases}$$

Since $\deg(x-a) = 1$ this implies that $r(x) = c$ is a constant. We can find the value of this constant by substituting $x = a$ to get

$$f(a) = (a-a)q(a) + c = c.$$

If $f(a) = 0$ then it follows that $c = 0$ and hence $f(x) = (x-a)q(x)$.

(b) If $f(x) \in \mathbb{F}[x]$ satisfies $f(a) = f(b) = 0$ for some $a, b \in \mathbb{F}$ with $a \neq b$, use part (a) to show that $f(x) = (x-a)(x-b)p(x)$ for some polynomial $p(x) \in \mathbb{F}[x]$. [Hint: From part (a) you already know that $f(x) = (x-a)q(x)$ for some $q(x)$.]

If $f(a) = 0$ and $a \in \mathbb{F}$ then from part (a) we have $f(x) = (x-a)q(x)$ for some $q(x) \in \mathbb{F}[x]$. Now suppose that we also have $f(b) = 0$ with $b \in \mathbb{F}$ and $b \neq a$. By substituting $x = b$ we obtain

$$0 = f(b) = (b-a)q(b),$$

which, since $b - a \neq 0$, implies that $q(b) = 0$. Then from part (a) we have $q(x) = (x-b)p(x)$ for some $p(x) \in \mathbb{F}[x]$, and putting everything together gives

$$f(x) = (x-a)q(x) = (x-a)(x-b)p(x).$$

Problem 3. Conjugation. Let $\mathbb{E} \supseteq \mathbb{F}$ be fields and let $* : \mathbb{E} \to \mathbb{E}$ be a function with the following properties:

(1) $a^* = a$ if and only if $a \in \mathbb{F}$
(2) $(a^*)^* = a$ for all $a \in \mathbb{E}$
(3) $(a+b)^* = a^* + b^*$ for all $a, b \in \mathbb{E}$
(4) $(ab)^* = a^* b^*$ for all $a, b \in \mathbb{E}$

(a) For all $f(x) \in \mathbb{F}[x]$ and $a \in \mathbb{E}$, show that $f(a)^* = f(a^*)$.

Let $f(x) = c_0 + c_1 x + c_2 x^2 \cdots + c_n x^n$ with $c_0, c_1, \ldots, c_n \in \mathbb{F}$. Then for all $a \in \mathbb{E}$,

$$\begin{aligned} f(a)^* &= (c_0 + c_1 a + c_2 a^2 + \cdots + c_n a^n)^* \\ &= c_0^* + (c_1 a)^* + (c_2 a^2)^* + \cdots + (c_n a^n)^* && (3) \\ &= c_0^* + c_1^* a^* + c_2^* (a^*)^2 + \cdots + c_n^* (a^*)^n && (4) \\ &= c_0 + c_1 a^* + c_2 (a^*)^2 + \cdots + c_n (a^*)^n && (1) \\ &= f(a^*). \end{aligned}$$

(b) Given $f(x) \in \mathbb{F}[x]$ use part (a) to show that the roots of $f(x)$ that are in $\mathbb{E}$ but not in $\mathbb{F}$ come in conjugate pairs.

For any $f(x) \in \mathbb{F}[x]$ and $a \in \mathbb{E}$ we will show that $f(a) = 0$ if and only if $f(a^*) = 0$. For one direction, suppose that $f(a) = 0$. Then from part (a) we have

$$f(a^*) = f(a)^* = 0^* = 0.$$

For the other direction, let $b = a^*$ so that $b^* = (a^*)^* = b$. Then it follows from the above argument that

$$f(a^*) = 0 \quad \Rightarrow \quad f(b) = 0 \quad \Rightarrow \quad f(b^*) = 0 \quad \Rightarrow \quad f(a) = 0.$$

[Remark: I guess I left this question a bit open-ended. To be very rigorous we should note that the elements of $\mathbb{E}$ that are not in $\mathbb{F}$ come in conjugate pairs of the form $\{a, a^*\}$. Indeed, since $a \notin \mathbb{F}$ we know from property (1) that $a \neq a^*$ so that $\{a, a^*\}$ is really a pair of elements. And no two pairs $\{a, a^*\}$ and $\{b, b^*\}$ can partially overlap because $a = b$ implies $a^* = b^*$ and $a = b^*$ implies $a^* = b$, so in either case we have $\{a, a^*\} = \{b, b^*\}$. Later we will use the following technical language: The "group" $\{\text{id}, *\}$ of automorphisms of $\mathbb{E}$ "partitions" the set $\mathbb{E}$ into "orbits".]

(c) For any $a \in \mathbb{E}$, show that the polynomial $(x-a)(x-a^*)$ has coefficients in $\mathbb{F}$. [Hint: Show that $a + a^*$ and aa^* are in $\mathbb{F}$.]

First we observe that $(a+a^*)^* = a^* + (a^*)^* = a^* + a = a + a^*$ from properties (2,3) and $(aa^*)^* = a^*(a^*)^* = a^*a = aa^*$ from properties (2,4), so that $a + a^* \in \mathbb{F}$ and $aa^* \in \mathbb{F}$ from property (1). It follows that

$$(x-a)(x-a^*) = x^2 - (a+a^*)x + aa^* \in \mathbb{F}[x].$$

(d) If a polynomial $f(x) \in \mathbb{F}[x]$ splits over $\mathbb{E}$, prove that it can be factored as a product of polynomials of degrees 1 and 2 with coefficients in $\mathbb{F}$. [Hint: Use parts (b),(c).]

If $f(x) \in \mathbb{F}[x]$ splits over $\mathbb{E}$ then from part (b) we can write

$$f(x) = \prod_i (x - r_i) \prod_j (x - a_j)(x - a_j^*)$$

for some $r_i \in \mathbb{F}$ and $a_j \in \mathbb{E}$ with $a_j \notin \mathbb{F}$. Then from part (c) we see that

$$f(x) = \prod_i (x - r_i) \prod_j (x^2 - (a_j + a_j)^* x + a_j a_j^*)$$

is a product of polynomials of degrees 1 and 2 with coefficients in $\mathbb{F}$.