Math 561/661 **Fall 2021**
Homework 1 **Drew Armstrong**

---

1. Working with Ring Axioms. Let $(R,+,\cdot,0,1)$ be a ring.[1] Recall that for any element $a\in R$ there exists a unique element $-a\in R$ such that $a+(-a)=0$.

(a) Show that $0a=0$. [Hint: Multiply both sides of $0+0=0$ by a.]
(b) Show that $-(-a)=a$. [Hint: Uniqueness.]
(c) Show that $a(-b)=(-a)b=-(ab)$. [Hint: Multiply both sides of $b+(-b)=0$ by a.]
(d) Show that $(-a)(-b)=ab$. [Hint: Combine parts (b) and (c).]

(a): From the definition of 0 we have $0+0=0$. Multiplying both sides by a and using the distributive axiom gives

$$\begin{aligned} 0+0&=0\\ (0+0)a&=0a\\ 0a+0a&=0a. \end{aligned}$$

Then we add the element $-0a$ to both sides to obtain

$$\begin{aligned} 0a+0a&=0a\\ (0a+0a)+(-0a)&=0a+(-0a)\\ 0a+[0a+(-0a)]&=0\\ 0a+0&=0\\ 0a&=0. \end{aligned}$$

(b): By definition we have $a+(-a)=0$ and rearranging gives $(-a)+a=0$. But we know that there exists a unique element $b\in R$ such that $(-a)+b=0$ and this element is called $-(-a)$. Since a is one such element then by uniqueness we must have $-(-a)=a$.[2]

(c): We multiply both sides of the equation $b+(-b)=0$ by a to obtain

$$\begin{aligned} b+(-b)&=0\\ a[b+(-b)]&=0a\\ ab+a(-b)&=0. && 0a=0 \text{ from part (a)} \end{aligned}$$

Then from the uniqueness of additive inverses it follows that $a(-b)=-(ab)$. The identity $(-a)b=-(ab)$ follows by reversing the roles of a and b.

(d): By combining parts (b) and (c) we obtain

$$\begin{aligned} (-a)(-b)&=-[a(-b)] && \text{part (c)}\\ &=-[-(ab)] && \text{part (c)}\\ &=ab. && \text{part (b)} \end{aligned}$$

[Remark: We could have taken these basic properties as axioms, but we didn't because it's not necessary. There is a general principle when it comes to axioms that we should use the minimum possible. I was very careful in this proof because this is the first homework problem of the course. As we go along I will not attempt to reduce every proof to the axioms.]

---

[1] We always assume that a ring has commutative multiplication.
[2] Full Details: $-(-a)=-(-a)+0=-(-a)+[(-a)+a]=[-(-a)+(-a)]+a=0+a=a$.

2. Complex Conjugation. Given a complex number $\alpha = a + bi \in \mathbb{C}$ we define the complex conjugate by $\alpha^* = a - bi$.

(a) For all $\alpha \in \mathbb{C}$ show that $\alpha^* = \alpha$ 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) If $f(x) \in \mathbb{R}[x]$ is a polynomial with real coefficients, show that the non-real complex roots of f come in conjugate pairs. [Hint: For all $\alpha \in \mathbb{C}$ show that $f(\alpha)^* = f(\alpha^*)$.]
(d) For any $\alpha \in \mathbb{C}$, show that the polynomial $(x-\alpha)(x-\alpha^*)$ has real coefficients.

(a): In class we showed that $a + bi = c + di$ implies that $a = c$ and $b = d$.[3] If $\alpha = a + bi$ and $\alpha = \alpha^*$ then we have $a + bi = a - bi$, which implies that $a = a$ and $b = -b$. The first of these equations tells us nothing; the second equation tells us that $2b = 0$ and hence $b = 0$. It follows that $\alpha = a + 0i$ is real. Conversely, if $\alpha = a + 0i$ is real then $\alpha^* = a - 0i = a + 0i = \alpha$.

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

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

and

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

(c): Consider a polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with real coefficients $a_0, \ldots, a_n \in \mathbb{R}$. For any $\alpha \in \mathbb{C}$ we want to show that $f(\alpha) = 0$ if and only if $f(\alpha^*) = 0$. In order to show this we first observe that for any $\alpha \in \mathbb{C}$ we have[4]

$$\begin{aligned}f(\alpha)^* &= (a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0)^* \\ &= a_n^*(\alpha^*)^n + a_{n-1}^*(\alpha^*)^{n-1} + \cdots + a_1^*\alpha^* + a_0^* && \text{part (b)} \\ &= a_n(\alpha^*)^n + a_{n-1}(\alpha^*)^{n-1} + \cdots + a_1\alpha^* + a_0 && \text{part (a)} \\ &= f(\alpha^*).\end{aligned}$$

If $f(\alpha) = 0$ then this implies that $f(\alpha^*) = f(\alpha)^* = 0^* = 0$ and if $f(\alpha^*) = 0$ then this implies that $f(\alpha) = [f(\alpha)^*]^* = f(\alpha^*)^* = 0^* = 0$.

(d): This problem was not assigned. I added it in the solutions because it is relevant for Problem 7. First we observe that

$$(x-\alpha)(x-\alpha^*) = x^2 - (\alpha+\alpha^*)x + \alpha\alpha^*.$$

[3] Proof: If $b \neq d$ then $i = (c-a)/(b-d)$ is real, which is a contradiction.

[4] Strictly speaking, we should use induction on top of part (b) to see that $(\alpha^n)^* = (\alpha^*)^n$.

There are two ways to show that these coefficients are real. *Direct Proof*: If $\alpha = a + bi$ then we have

$$\alpha + \alpha^* = (a + bi) + (a - bi) = 2a + 0i \in \mathbb{R}$$

and

$$\alpha\alpha^* = (a + bi)(a - bi) = (a^2 + b^2) + 0i \in \mathbb{R}.$$

Elegant Proof: From part (b) we have

$$(\alpha + \alpha^*)^* = \alpha^*\alpha^{**} = \alpha^* + \alpha = \alpha + \alpha^*$$

and

$$(\alpha\alpha^*) = \alpha^*\alpha^{**} = \alpha^*\alpha = \alpha\alpha^*,$$

hence from part (a) we have $\alpha + \alpha^* \in \mathbb{R}$ and $\alpha\alpha^* \in \mathbb{R}$.

3. Absolute Value of Complex Numbers. Given a complex number $\alpha = a + bi \in \mathbb{C}$ we define the absolute value by $|\alpha| = +\sqrt{a^2 + b^2}$.

(a) Show that $\alpha = 0$ if and only if $|\alpha| = 0$. [Hint: For all $a \in \mathbb{R}$ we have $a^2 \geq 0$.]
(b) Show that $\alpha\alpha^* = |\alpha|^2$.
(c) For all $\alpha, \beta \in \mathbb{C}$ show that $|\alpha\beta| = |\alpha||\beta|$. [Hint: Part (b) gives a shortcut.]
(d) For all $\alpha, \beta \in \mathbb{C}$ show that $\alpha\beta = 0$ implies $\alpha = 0$ or $\beta = 0$. [Hint: Use parts (a,c).]

(a): If $\alpha = 0 + 0i$ then $|\alpha|^2 = 0^2 + 0^2 = 0$ and hence $|\alpha| = 0$. Conversely, let $\alpha = a + bi$. If $|\alpha| = 0$ then $0 = |\alpha|^2 = a^2 + b^2$, which implies that $a^2 = -b^2$. If $a \neq 0$ then since a, b are real this shows that a strictly positive number a^2 is equal to a non-negative number $-b^2$, which is a contradiction. It follows that $a = 0$ hence also $b^2 = -a^2 = -0^2 = 0$ and $b = 0$. We conclude that $\alpha = 0 + 0i$ as desired.

(b): If $\alpha = a + bi$ then we have

$$\alpha\alpha^* = (a + bi)(a - bi) = (a^2 + b^2) + 0i = |\alpha|^2.$$

(c): For all $\alpha, \beta \in \mathbb{C}$, part (b) and 2(b) imply that

$$|\alpha\beta|^2 = (\alpha\beta)(\alpha\beta)^* = \alpha\beta\alpha^*\beta^* = (\alpha\alpha^*)(\beta\beta^*) = |\alpha|^2|\beta|^2.$$

Then taking positive real square roots gives $|\alpha\beta| = |\alpha||\beta|$.

(d): The hint that I gave for this problem is a bit silly because we already know from class that $\mathbb{C}$ is a field. *Here is the proof using the hint:* Suppose that $\alpha\beta = 0$ so from part (c) we have that $|\alpha||\beta| = |\alpha\beta| = 0$. Since $|\alpha|$ and $|\beta|$ are real numbers this implies that $|\alpha| = 0$ or $|\beta| = 0$, which from part (a) shows that $\alpha = 0$ or $\beta = 0$. *And here is the proof using the fact that $\mathbb{C}$ is a field:* Suppose that $\alpha\beta = 0$. If $\beta \neq 0$ then there exists $\beta^{-1} \in \mathbb{C}$ such that $\beta\beta^{-1} = 1$, and it follows that

$$\begin{aligned} \alpha\beta &= 0 \\ \alpha\beta\beta^{-1} &= 0\beta \\ \alpha &= 0. \end{aligned}$$

If $\alpha \neq 0$ then a similar argument shows that $\beta = 0$. Hence we must have $\alpha = 0$ or $\beta = 0$.[5]

4. Descartes' Factor Theorem. Let $\mathbb{F}$ be a field and let $\mathbb{F}[x]$ be the ring of polynomials

$$\mathbb{F}[x] = \{a_0 + a_1 x + \cdots + a_n x^n : a_0, \ldots, a_n \in \mathbb{F}, n \geq 0\}.$$

[5]The key observation I want to make is that this property is not obvious from the definition of $\mathbb{C}$. It relies on properties of complex conjugation and absolute value.

If $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ with $a_n \neq 0$ then we write $\deg(f) = n$. The zero polynomial does not have a degree.

(a) Show that $\deg(fg) = \deg(f) + \deg(g)$ for all nonzero polynomials $f(x), g(x) \in \mathbb{F}[x]$.

(b) Suppose that a nonzero polynomial $f(x) \in \mathbb{F}[x]$ satisfies $f(\alpha) = 0$ for some $\alpha \in \mathbb{F}$. In this case prove that we have $f(x) = (x - \alpha)g(x)$ for some polynomial $g(x)$ with $\deg(g) = \deg(f) - 1$. [Hint: By long division there exist polynomials $q(x), r(x) \in \mathbb{F}[x]$ with $f(x) = (x - \alpha)q(x) + r(x)$, such that $r(x)$ is a constant.]

(c) Use part (b) to prove that a polynomial $f(x) \in \mathbb{F}[x]$ of degree n has **at most n distinct roots in $\mathbb{F}$**. [Hint: If $f(\alpha) = 0$ then $f(x) = (x - \alpha)g(x)$ for some polynomial of degree $n - 1$. What happens if $f(\beta) = 0$ for some $\beta \neq \alpha$? Use induction.]

(a): Suppose that $\deg(f) = m$ and $\deg(g) = n$ so that

$$\begin{aligned} f(x) &= a_m x^m + \cdots + a_1 x + a_0, \\ g(x) &= b_n x^n + \cdots + b_1 x + b_0, \end{aligned}$$

for some coefficients $a_0, \ldots, a_m, b_0, \ldots, b_n \in \mathbb{F}$ with $a_m \neq 0$ and $b_n \neq 0$. By definition of polynomial multiplication we have[6]

$$f(x)g(x) = a_m b_n x^{m+n} + \text{ lower degree terms.}$$

Then since $a_m \neq 0$ and $b_n \neq 0$ we have $a_m b_n \neq 0$ which implies that

$$\deg(fg) = m + n = \deg(f) + \deg(g).$$

(b): Consider a polynomial $f(x) \in \mathbb{F}[x]$ and a constant $\alpha \in \mathbb{F}$. If $f(x) = (x - \alpha)g(x)$ for some polynomial $g(x) \in \mathbb{F}[x]$ then we must have

$$f(\alpha) = (\alpha - \alpha)g(\alpha) = 0g(\alpha) = 0.$$

Conversely, let us suppose that $f(\alpha) = 0$. First we apply long division to obtain a quotient and remainder $q(x), r(x) \in \mathbb{F}[x]$ such that $f(x) = (x - \alpha)q(x) + r(x)$, where either $r(x) = 0$ or $r(x)$ has degree strictly less than $(x - \alpha)$. Since $x - \alpha$ has degree 1 this implies that either $r(x) = 0$ or $r(x)$ has degree zero, i.e., is a non-zero constant. In either case we have $r(x) = c$ for some $c \in \mathbb{F}$. Now we substitute $x = \alpha$ to obtain

$$0 = f(\alpha) = (\alpha - \alpha)q(\alpha) + c = c,$$

so that $f(x) = (x - \alpha)q(x)$ as desired. The fact that $\deg(q) = \deg(f) - 1$ follows from (a).

(c): **Theorem:** Any polynomial $f(x) \in \mathbb{F}[x]$ of degree $n \geq 0$ has at most n distinct roots in $\mathbb{F}$.
Proof by Induction: If $n = 0$ then $f(x) = c$ for some nonzero constant $c \in \mathbb{F}$, which implies that $f(x)$ has no roots, as desired. So let us suppose that $n \geq 1$ and assume for induction that every polynomial of degree $n - 1$ has at most $n - 1$ roots in $\mathbb{F}$. If $f(x)$ has no roots then we are done. Otherwise, we may suppose that $f(\alpha) = 0$ for some $\alpha \in \mathbb{F}$, so from part (b) we have $f(x) = (x - \alpha)g(x)$ for some $g(x) \in \mathbb{F}[x]$ of degree $n - 1$. If $\beta \in \mathbb{F}$ is **any other root** of $f(x)$ (i.e., if $f(\beta) = 0$ and $\beta \neq \alpha$) then substituting gives

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

which implies that β is a root of $g(x)$. But $g(x)$ has at most $n - 1$ roots in $\mathbb{F}$. Therefore $f(x)$ has at most $1 + (n - 1) = n$ roots in $\mathbb{F}$ □

[6] It is possible to be more precise about this but I don't want to.

[Remark: This theorem goes back to Descartes' *Geometry* (1631) and is one of the most fundamental results in algebra. I'm sure you've seen it before but you may not have seen a proof.]

5. Leibniz' Mistake. In 1702 Gottfried Leibniz claimed that the polynomial x^4+1 cannot be factored as a product of smaller polynomials with real coefficients.

(a) Use the polar form to find all of the complex 4th roots of -1.

(b) Use this to factor the polynomial x^4+1 and show that Leibniz was wrong. [Hint: Group the four roots into complex conjugate pairs.]

[Remark: It follows from Problem 4 that a complex number can have **at most four 4th roots in $\mathbb{C}$**. If we can find four distinct complex 4th roots then we will have all of them.]

(a): First note that $\alpha := -1 = re^{i\theta}$ with $r = 1 > 0$ and $\theta = \pi$. Note that 1 is the unique positive 4th root of 1. Thus the "principal" 4th roof of α is $\alpha' := 1e^{i\theta/4} = e^{i\pi/4}$. If $\omega = e^{2\pi i/4} = e^{\pi i/2}$ then I claim that the 4th roots of -1 are[7]

$$\begin{array}{rcccccc} \alpha' &=& e^{\pi i/4} &=& \cos(\pi/4) + i\sin(\pi/4) &=& (1+i)/\sqrt{2}, \\ \alpha'\omega &=& e^{3\pi i/4} &=& \cos(3\pi/4) + i\sin(3\pi/4) &=& (-1+i)/\sqrt{2}, \\ \alpha'\omega^2 &=& e^{5\pi i/4} &=& \cos(5\pi/4) + i\sin(5\pi/4) &=& (-1-i)/\sqrt{2}, \\ \alpha'\omega^3 &=& e^{7\pi i/4} &=& \cos(7\pi/4) + i\sin(7\pi/4) &=& (1-i)/\sqrt{2}. \end{array}$$

Indeed, since $(\alpha')^n = \alpha$ and $\omega^4 = e^{2\pi i} = 1$ we have

$$(\alpha'\omega^k)^n = (\alpha')^n(\omega^n)^k = \alpha \cdot 1^k = \alpha \quad \text{for any integer } k.$$

We have four four distinct 4roots of -1, and hence all of them.

(b): From Descartes' Theorem we may use these fourth roots to factor the polynomial over the complex numbers:

$$x^4+1 = \left(x - \frac{1+i}{\sqrt{2}}\right)\left(x - \frac{-1+i}{\sqrt{2}}\right)\left(x - \frac{-1-i}{\sqrt{2}}\right)\left(x - \frac{1-i}{\sqrt{2}}\right).$$

We observe that these roots come in complex-conjugate pairs, as predicted by Problem 2(c). By grouping these pairs and expanding, we obtain a factorization of x^4+1 over the **real numbers**:[8]

$$\begin{aligned} x^4+1 &= \left[\left(x - \frac{1+i}{\sqrt{2}}\right)\left(x - \frac{1-i}{\sqrt{2}}\right)\right]\left[\left(x - \frac{-1+i}{\sqrt{2}}\right)\left(x - \frac{-1-i}{\sqrt{2}}\right)\right] \\ &= (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1). \end{aligned}$$

[Remark: Leibniz (1702) did not find this factorization because he did not have a geometric understanding of the complex numbers.]

[7] Geometrically, these four points in the complex plane form a square centered at the origin.

[8] For any complex number $\alpha \in \mathbb{C}$ we observe that the polynomial $(x-\alpha)(x-\alpha^*) = x^2 - (\alpha+\alpha^*)x + \alpha\alpha^*$ has real coefficients because $\alpha + \alpha^*$ and $\alpha\alpha^*$ are real.