Math 461 **Spring 2015**
Homework 2 **Drew Armstrong**

---

1. Let $\mathbb{F}$ be a field and consider two polynomials $f(x), g(x) \in \mathbb{F}[x]$.
(a) If $f(x)$ and $g(x)$ are both nonzero, prove that $\deg(fg) = \deg(f) + \deg(g)$.
(b) How should you define the "degree" of the zero polynomial so that the result in part (a) remains true even when one or both of $f(x)$ and $g(x)$ is zero?

I'll give two proofs for part (a): a human proof and a formal proof. You are free to use human-style proofs but be warned that they are riskier.

Human Proof: Let $f(x)$ be a polynomial of degree m with leading term $a_m x^m$ ($a_m \neq 0$) and let $g(x)$ be a polynomial of degree n with leading term $b_n x^n$ ($b_n \neq 0$). Note that the product equals $f(x)g(x) = (a_m b_n)x^{m+n} +$ lower order terms. Since $a_m \neq 0$ and $b_n \neq 0$ imply $a_m b_n \neq 0$ we conclude that $f(x)g(x)$ has degree $m+n$. ///

Formal Proof: Consider polynomials $f(x) = \sum_{k\geq 0} a_k x^k$ and $g(x) = \sum_{k\geq 0} b_k x^k$. We assume that $f(x)$ has degree m (so that $a_m \neq 0$ and $a_i = 0$ for all $i > m$) and $g(x)$ has degree n (so that $b_n \neq 0$ and $b_j = 0$ for all $j > n$). Note that the product is

$$f(x)g(x) = \sum_{k\geq 0} \left(\sum_{i+j=k} a_i b_j \right) x^k.$$

We claim that the degree of $f(x)g(x)$ is $m+n$. To see this, first note that the coefficient of x^{m+n} in $f(x)g(x)$ is $a_m b_n$, which is nonzero because $a_m \neq 0$ and $b_n \neq 0$. Then note that the coefficient of x^k in $f(x)g(x)$ is zero for all $k > m+n$. Indeed, if $i+j = k > m+n$ then we must have either $i > m$ or $j > n$ (contrapositive: if $i \leq m$ and $j \leq n$ then $i+j \leq m+n$). If either $i > m$ (hence $a_i = 0$) or $j > n$ (hence $b_j = 0$) then the product $a_i b_j$ is zero. Hence the whole sum $\sum_{i+j=k} a_i b_j$ is zero. ///

For part (b), suppose that we can define $\deg(0)$ so that the result of part (a) is still true. Then for any polynomial $f(x) \in \mathbb{F}[x]$ we would have

$$\deg(0) = \deg(0 \cdot f(x)) = \deg(0) + \deg(f(x)).$$

Subtracting $\deg(0)$ from both sides gives $\deg(f(x)) = 0$. We conclude that **every** polynomial has degree zero. Oops. The only alternative is to do something weird like define $\deg(0) = \infty$ or $\deg(0) = -\infty$. When people do this they prefer $\deg(0) = -\infty$ because then they can say that $\deg(0) < \deg(f(x))$ for all nonzero $f(x) \in \mathbb{F}[x]$, which is nice. In particular, this simplifies the statement of the Division Theorem for Polynomials: Given $f(x), g(x) \in \mathbb{F}[x]$ with $g(x)$ nonzero, there exist unique polynomials $q(x), r(x) \in \mathbb{F}[x]$ such that

- $f(x) = q(x)g(x) + r(x)$, and
- $\deg(r) < \deg(g)$.

Isn't that nice?

2. Let $\mathbb{F}$ be a field with **finitely** many elements. Prove that there must exist two non-equal polynomials (i.e., with different coefficients) that yield equal functions $\mathbb{F} \to \mathbb{F}$. [Hint: How many different polynomials are there? How many different functions?]

This time I won't give two proofs; I'll just aim for the middle.

Proof: If $\mathbb{F}$ is a finite field, note that the number of possible functions $\mathbb{F} \to \mathbb{F}$ is **finite**. Indeed, if X and Y are any finite sets then the number of possible functions $X \to Y$ is $\#Y^{\#X}$. So the number of functions $\mathbb{F} \to \mathbb{F}$ is $\#\mathbb{F}^{\#\mathbb{F}}$, which is finite.

On the other hand, the size of $\mathbb{F}[x]$ is **infinite**. Indeed, it contains the polynomials $1, x, x^2, x^3, x^4, \ldots$, which are all distinct. Since there are infinitely many different polynomials and only finitely many different functions, we conclude that there must exist two different polynomials that determine the same function. ///

[That being said, it turns out that over an **infinite** field, two different polynomials always determine different functions. We will mostly (always) work with infinite fields in this class.]

3. Let $\mathbb{F}$ be a field and consider the ring of polynomials $\mathbb{F}[x]$. Apply Descartes' Factor Theorem to prove the following statement: If $f(x) \in \mathbb{F}[x]$ has degree n, then $f(x)$ has **at most** n distinct roots in $\mathbb{F}$. [Hint: Use induction.]

OK, this one needs two proofs.

Human Proof: Note that a polynomial of degree zero is just a nonzero constant, so it certainly has no roots. Next let $f(x) \in \mathbb{F}[x]$ have degree $n \geq 1$. If $f(x)$ has no roots in $\mathbb{F}$ then there is nothing to show. Otherwise, suppose that $f(\alpha) = 0$ for some $\alpha \in \mathbb{F}$. By Descartes' Factor Theorem and Problem 1(a) we can write

$$f(x) = (x - \alpha)g(x)$$

where $g(x) \in \mathbb{F}[x]$ has degree $n - 1$. If $0 = f(\beta) = (\beta - \alpha)g(\beta)$ then we must have either $\beta = \alpha$ or $g(\beta) = 0$. That is, the roots of $f(x)$ are just the roots of $g(x)$ together with α. But by induction we can assume that $g(x)$ has at most $n - 1$ distinct roots. It follows that $f(x)$ has at most n distinct roots. ///

[In a real world proof by induction we assume that the reader understands how induction works, so it is sufficient to focus on the mathematical details. If you write your proof like this it needs to be perfect. Mistakes in an informal proof will lose more points than mistakes in a formal proof.]

Formal Proof: Let $\mathbb{F}$ be a field and consider the statement $P(n) =$"any polynomial $f(x) \in \mathbb{F}[x]$ of degree n has at most n distinct roots in $\mathbb{F}$". We will prove by induction that $P(n)$ is a true statement for all $n \geq 0$.

- *Base Case.* First note that $P(0)$ is true. Indeed, a polynomial of degree zero is just a nonzero constant, and a nonzero constant function has no roots.
- *Induction Step.* Next we **assume** for induction that $P(n)$ is a true statement for $n = 0, 1, \ldots, k$. We will show in this case that $P(k+1)$ is also true. To do this, consider an arbitrary polynomial $f(x) \in \mathbb{F}[x]$ of degree $k+1$. If $f(x)$ has no roots in $\mathbb{F}$ then we are done. Otherwise, suppose that $f(\alpha) = 0$ for some $\alpha \in \mathbb{F}$. Using Descartes' Factor Theorem we can write

  $$f(x) = (x - \alpha)g(x)$$

  for some polynomial $g(x) \in \mathbb{F}[x]$. Then Problem 1(a) tells us that

  $$k = \deg(f(x)) = \deg(x - \alpha) + \deg(g(x)) = 1 + \deg(g(x)),$$

  hence $g(x)$ has degree k. But we have assumed that $P(k)$ is a true statement, so that $g(x)$ has at most k distinct roots in $\mathbb{F}$. Note that any root $f(\beta) = 0$ satisfies $(\beta - \alpha)g(\beta) = 0$ so that either $\beta - \alpha = 0$ (i.e., $\beta = \alpha$) or $g(\beta) = 0$ (i.e., β is a root of $g(x)$). Since $g(x)$ has at most k distinct roots in $\mathbb{F}$, we conclude that $f(x)$ has at most $k + 1$ distinct roots in $\mathbb{F}$. Thus $P(k+1)$ is true.

By the Principle of Induction (which is really an axiom) we conclude that the statement $P(n)$ is true for all $n \geq 0$. ///

4. Assume that the cubic equation $ax^3 + bx^2 + cx + d = 0$ has three distinct roots, called r, s, and t. Give a formula for $rs + rt + st$ in terms of the coefficients a, b, c, and d.

First we define the polynomial $f(x) = ax^3 + bx^2 + cx + d \in \mathbb{F}[x]$. I don't know where the coefficients live; just some field $\mathbb{F}$. We might as well also assume that $r, s, t \in \mathbb{F}$. Since $f(r) = 0$, Descartes' Factor Theorem says that

$$f(x) = (x - r)g(x),$$

where $g(x) \in \mathbb{F}[x]$ has degree 2. Next, since $f(s) = 0$ we have $(s - r)g(s) = 0$. Since $s \neq r$ by assumption, we have $g(s) = 0$ and Descartes' Factor Theorem says

$$f(x) = (x - r)(x - s)h(x),$$

where $h(x) \in \mathbb{F}[x]$ has degree 1. Finally, since $f(t) = 0$ we have $(t - r)(t - s)h(t) = 0$. Since $t \neq r$ and $t \neq s$ by assuption, this implies $h(t) = 0$, so Descartes' Factor Theorem says

$$f(x) = (x - r)(x - s)(x - t)w(x),$$

where $w(x) \in \mathbb{F}[x]$ has degree 0. But a polynomial of degree zero is just a nonzero constant. Which constant is this? By comparing the leading terms we see that $w(x) = a$, hence

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

Comparing coefficients on both sides gives

$$rs + rt + st = \frac{c}{a}.$$

///

5. Prove that $\sqrt[3]{7 + \sqrt{50}} + \sqrt[3]{7 - \sqrt{50}} = 2$. [Hint: Maybe the cube roots of $7 + \sqrt{50}$ and $7 - \sqrt{50}$ have the form $a + b\sqrt{2}$, where a and b are small whole numbers.]

This is a trial-and-error kind of problem. The hint says to consider numbers of the form

$$(a + b\sqrt{2})^3 = a^3 + 3a^2b\sqrt{2} + 3ab^2(\sqrt{2})^2 + b^3(\sqrt{2})^3 = (a^3 + 6ab^2) + (3a^2b + 2b^3)\sqrt{2}.$$

We are looking for small whole numbers such that $a^3 + 6ab^2 = 7$ and $3a^2b + 2b^3 = \pm 5$. In general this kind of problem can be hard, but not this time. Check that the values $a = 1$ and $b = \pm 1$ work:

$$\begin{aligned} (1 + \sqrt{2})^3 &= 7 + 5\sqrt{2} = 7 + \sqrt{50}, \\ (1 - \sqrt{2})^3 &= 7 - 5\sqrt{2} = 7 - \sqrt{50}. \end{aligned}$$

We conclude that

$$\sqrt[3]{7 + \sqrt{50}} + \sqrt[3]{7 - \sqrt{50}} = (1 + \sqrt{2}) + (1 - \sqrt{2}) = 2.$$

At least, that's one valid interpretation of the expression. ///

6. Define a function $f : \mathbb{C} \to \mathrm{M}_{2\times 2}(\mathbb{R})$ from complex numbers to real 2×2 matrices by setting

$$f(a + ib) := \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

For any complex numbers $u, v \in \mathbb{C}$ verify the following:

(a) $f(u+v) = f(u) + f(v)$
(b) $f(uv) = f(u)f(v)$
(c) $|u|^2 = \det f(u)$.

(The operations on the right hand side are matrix addition, matrix multiplication, and matrix determinant.)

Let $u = a + ib$ and $v = c + id$ where $a, b, c, d \in \mathbb{R}$. For part (a) we have

$$\begin{aligned} f(a+ib) + f(c+id) &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \\ &= \begin{pmatrix} a+c & -(b+d) \\ b+d & a+c \end{pmatrix} \\ &= f((a+c) + i(b+d)) \\ &= f((a+ib) + (c+id)). \end{aligned}$$

For part (b) we have

$$\begin{aligned} f(a+ib)f(c+id) &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \\ &= \begin{pmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{pmatrix} \\ &= f((ac-bd) + i(ad+bc)) \\ &= f((a+ib)(c+id)). \end{aligned}$$

For part (c) we note that $|a+ib|^2 = a^2 + b^2$ and $\det \left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right) = a^2 + b^2$. ///

[So what? In this problem you showed that the function $f : \mathbb{C} \to \mathrm{M}_{2\times 2}(\mathbb{R})$ is a **homomorphism** (homo=similar, morphism=structure). In this case, f is a **ring homomorphism** because it respects the ring operations. But more is true; to get technical, this f is a homomorphism of "normed $\mathbb{R}$-algebras". This homomorphism is injective but not surjective because not every 2×2 real matrix has the form $\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$. Those that do comprise a **sub-algebra** of $\mathrm{M}_{2\times 2}(\mathbb{R})$ **isomorphic** to $\mathbb{C}$ (iso=same, morphism=structure). More abstract courses in algebra will talk about homomorphisms every single day.]