Math 461 F **Spring 2011**
Homework 5 Solutions **Drew Armstrong**

Problems.

A.1. Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{R}[x]$. If n is **even**, with $a_n > 0$ and $a_0 < 0$, **prove** that $f(x)$ has at least two real roots. (Hint: Intermediate value theorem.)

Consider the graph of $f(x)$. Since $f(0) = a_0 < 0$, we see that the y-intercept of the graph is negative. On the other hand, since $a_n > 0$ and n is even, the leading term $a_n x^n$ is positive for any x. For $|x|$ large, the term $a_n x^n$ will dominate, and so we have

$$\lim_{x\to-\infty} f(x) = +\infty \qquad \text{and} \qquad \lim_{x\to+\infty} f(x) = +\infty.$$

If $\lim_{x\to-\infty} f(x) = +\infty$, there must exist some number $\alpha < 0$ where $f(\alpha) > 0$. Since $f(0) = a_0 < 0$, the Intermediate Value Theorem implies that there exists some $\alpha < \beta < 0$ such that $f(\beta) = 0$. Similarly, there is some value $0 < a$ where $f(a)$ and so there exists $0 < b < a$ with $f(b) = 0$. We have found two real roots.

A.2. Leibniz (1702) claimed that $x^4 + a^4$ (for $a \in \mathbb{R}$) cannot be factored over $\mathbb{R}$. (In modern language, he claimed that $x^4 + a^4 \in \mathbb{R}[x]$ is irreducible.) **Prove him wrong.** (Hint: What are the fourth roots of $-a^4$?)

First we will solve the equation $x^4 + a^4$, or $x^4 = -a^4$. Since $a^4 > 0$ we can write $-a^4 = a^4 \operatorname{cis}(\pi)$ in polar form. Thus the fourth roots of $-a^4$ will have length $|a|$ and angles $(\pi + 2\pi k)/4$ for $k \in \mathbb{Z}$. In other words,

$$\begin{aligned}
\sqrt[4]{-a^4} &= \{|a| \operatorname{cis}(\pi/4), |a| \operatorname{cis}(3\pi/4), |a| \operatorname{cis}(5\pi/4), |a| \operatorname{cis}(7\pi/4)\} \\
&= \left\{ \frac{|a|}{\sqrt{2}}(1+i), \frac{|a|}{\sqrt{2}}(-1+i), \frac{|a|}{\sqrt{2}}(-1-i), \frac{|a|}{\sqrt{2}}(1-i) \right\}.
\end{aligned}$$

By grouping the roots into conjugate pairs, we conclude that

$$\begin{aligned}
x^4 + a^4 &= \left(x - \frac{|a|}{\sqrt{2}}(1+i)\right)\left(x - \frac{|a|}{\sqrt{2}}(1-i)\right)\left(x - \frac{|a|}{\sqrt{2}}(-1+i)\right)\left(x - \frac{|a|}{\sqrt{2}}(-1-i)\right) \\
&= \left(x^2 - 2\frac{|a|}{\sqrt{2}}x + |a|^2\right)\left(x^2 + 2\frac{|a|}{\sqrt{2}}x + |a|^2\right) \\
&= \left(x^2 - |a|\sqrt{2}\,x + a^2\right)\left(x^2 + |a|\sqrt{2}\,x + a^2\right) \\
&= \left(x^2 - a\sqrt{2}\,x + a^2\right)\left(x^2 + a\sqrt{2}\,x + a^2\right)
\end{aligned}$$

We have succeeded in factoring $x^4 + a^4$ into two real quadratics. That is, **Leibniz was wrong**.

Note: In the case $a = \sqrt{2}$ we recover the result from **Exam 1, Problem 3**:

$$x^4 + (\sqrt{2})^4 = x^4 + 4 = (x^2 - 2x + 2)(x^2 + 2x + 2).$$

A.3. Nicolaus Bernoulli (1742) claimed in a letter to Euler that

$$f(x) = x^4 - 4x^3 + 2x^2 + 4x + 4$$

does not factor over $\mathbb{R}$. Euler responded (1743) that $f(x)$ has roots $1 \pm \alpha/2$ and $1 \pm \overline{\alpha}/2$, where

$$\alpha = \sqrt{2\sqrt{7} + 4} + i\sqrt{2\sqrt{7} - 4}.$$

Use this information to **prove Bernoulli wrong**.

First note that $\overline{1+\alpha/2} = 1+\overline{\alpha}/2$ and $\overline{1-\alpha/2} = 1-\overline{\alpha}/2$. Then grouping the roots into conjugate pairs gives

$$\begin{aligned} f(x) &= (x-(1+\alpha/2))(x-(1+\overline{\alpha}/2))(x-(1-\alpha/2))(x-(1-\overline{\alpha}/2)) \\ &= \left(x - \left(2+\frac{\alpha+\overline{\alpha}}{2}\right)x + \left(1+\frac{\alpha+\overline{\alpha}}{2}+\frac{\alpha\overline{\alpha}}{4}\right)\right)\left(x - \left(2+\frac{\alpha+\overline{\alpha}}{2}\right)x + \left(1+\frac{\alpha+\overline{\alpha}}{2}+\frac{\alpha\overline{\alpha}}{4}\right)\right) \end{aligned}$$

Since $\alpha+\overline{\alpha}$ and $\alpha\overline{\alpha}$ are always real for any $\alpha \in \mathbb{C}$, we have factored $f(x)$ into two real quadratics. If you like, you can follow Euler to get the explicit formulas. The first of the two quadratic factors is

$$\left(x - \left(2+\sqrt{2\sqrt{7}+4}\right)x + \left(1+\sqrt{7}+\sqrt{2\sqrt{7}+4}\right)\right)$$

A.4. Given a polynomial $p(x) \in \mathbb{C}[x]$ with complex coefficients, we define its conjugate polynomial $\overline{p}(x)$ by

$$\overline{p}(z) := \overline{p(\overline{z})} \qquad \text{for all } z \in \mathbb{C}.$$

This has the effect of conjugating the coefficients. **Prove** that the polynomial $f(x) = p(x)\overline{p}(x)$ has **real** coefficients.

Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$, so that $\overline{p}(x) = \overline{a_n}x^n + \overline{a_{n-1}}x^{n-1} + \cdots + \overline{a_1}x + \overline{a_0}$. Note that each term of the product $f(x) = p(x)\overline{p}(x)$ is equal to the product of some term from $p(x)$ and some term from $\overline{p}(x)$. That is, the the x^k term of $f(x)$ looks like

$$a_0x^0\overline{a_k}x^k + a_1x^1\overline{a_{k-1}}x^{k-1} + \cdots + a_{k-1}x^{k-1}\overline{a_1}x^1 + a_kx^k\overline{a_0}x^0.$$

In other words, the coefficient of x^k in $f(x)$ is

$$a_0\overline{a_k} + a_1\overline{a_{k-1}} + a_2\overline{a_{k-2}} + \cdots + a_{k-2}\overline{a_2} + a_{k-1}\overline{a_1} + a_k\overline{a_0}.$$

Now let us conjugate this coefficient to get

$$\begin{aligned} &\overline{a_0\overline{a_k} + a_1\overline{a_{k-1}} + a_2\overline{a_{k-2}} + \cdots + a_{k-2}\overline{a_2} + a_{k-1}\overline{a_1} + a_k\overline{a_0}} \\ &= \overline{a_0}a_k + \overline{a_1}a_{k-1} + \overline{a_2}a_{k-2} + \cdots + \overline{a_{k-2}}a_2 + \overline{a_{k-1}}a_1 + \overline{a_k}a_0 \\ &= a_k\overline{a_0} + a_{k-1}\overline{a_1} + a_{k-2}\overline{a_2} + \cdots + a_2\overline{a_k - 2} + a_1\overline{a_{k-1}} + a_0\overline{a_k} \\ &= a_0\overline{a_k} + a_1\overline{a_{k-1}} + a_2\overline{a_{k-2}} + \cdots + a_{k-2}\overline{a_2} + a_{k-1}\overline{a_1} + a_k\overline{a_0}. \end{aligned}$$

Recall that a complex number α is real if and only if $\overline{\alpha} = \alpha$. Since the coefficient of x^k is equal to its own conjugate, we conclude that it is real. This is true for every coefficient of $f(x)$.

For the following problems you should use Proposition 6.10 in the text, which says: If $G(x)$ is a greatest common divisor (common divisor with **largest degree**) of $A(x)$ and $B(x)$ over some field $\mathbb{F}$, then **there exist** polynomials $M(x)$ and $N(x)$ over $\mathbb{F}$ such that

$$A(x)M(x) + B(x)N(x) = G(x).$$

A.5. Prove: If $H(x)$ is any other common divisor of $A(x)$ and $B(x)$ then $H(x)$ divides $G(x)$. If $H(x)$ also has largest degree, then $H(x) = cG(x)$ for some nonzero constant $c \in \mathbb{F}$. Hence we can say that "the" greatest common divisor of $A(x)$ and $B(x)$ is **unique** up to nonzero constant multiples.

Suppose that $G(x)$ and $H(x)$ are both gcd's for $A(x)$ and $B(x)$. That is, they are both common divisors with largest possible degree, say n. How different could they be? Using Prop 6.10 in the text, there exist polynomials $M(x)$ and $N(x)$ such that

$$A(x)M(x) + B(x)N(x) = G(x).$$

But since $H(x)$ is a common divisor of $A(x)$ and $B(x)$ by definition, there exist polynomials $\alpha(x)$ and $\beta(x)$ such that $A(x) = H(x)\alpha(x)$ and $B(x) = H(x)\beta(x)$. Substituting this into the original equation gives

$$\begin{aligned} H(x)\alpha(x)M(x) + H(x)\beta(x)N(x) &= G(x) \\ H(x)(\alpha(x)M(x) + \beta(x)N(x)) &= G(x) \end{aligned}$$

We conclude that $H(x)$ divides $G(x)$. Let $Q(x) = \alpha(x)M(x)+\beta(x)N(x)$ so that $H(x)Q(x) = G(x)$. Equating degrees of these two polynomials gives $\deg(Q)+\deg(H) = \deg(G)$. But we have $\deg(H) = \deg(G) = n$ by assumption, which implies that $\deg(Q) = 0$. The polynomials of degree zero are precisely the nonzero constants $k \neq 0 \in \mathbb{F}$. Hence $kH(x) = G(x)$, or $H(x) = \frac{1}{k}G(x)$. We conclude that any two gcd's for $A(x)$ and $B(x)$ differ by multiplication by a nonzero constant.

Note: If we expand the definition to say that a gcd must be monic (have leading coefficient equal to 1), then this result implies that every two polynomials have a **unique** greatest common divisor.

A.6. Euclid's Lemma for Polynomials. Let $P(x)$ be an irreducible polynomial over $\mathbb{F}$ (it cannot be factored into two polynomials of positive degree over $\mathbb{F}$) and suppose that $P(x)$ divides a product $F(x)G(x)$. In this case, **prove** that $P(x)$ must divide either $F(x)$ or $G(x)$ (or both).

Let $P(x)$ be irreducible and suppose that $P(x)$ divides $F(x)G(x)$. If $P(x)$ divides either of the factors we are done. So suppose without loss of generality that $P(x)$ does not divide $F(x)$. What could the gcd of $P(x)$ and $F(x)$ be? Since the gcd divides $P(x)$ it can be only 1 or $P(x)$. But the gcd must also divide $F(x)$ so we conclude that $\gcd(P(x), F(x)) = 1$. By Prop 6.10 there exist polynomials $M(x)$ and $N(x)$ such that

$$P(x)M(x) + F(x)N(x) = 1.$$

Multiply this equation by $G(x)$ and use the fact that $P(x)Q(x) = F(x)G(x)$ for some $Q(x)$ to conclude that

$$\begin{aligned} P(x)M(x)G(x) + F(x)G(x)N(x) &= G(x) \\ P(x)M(x)G(x) + P(x)Q(x)N(x) &= G(x) \\ P(x)(M(x)G(x) + Q(x)N(x)) &= G(x). \end{aligned}$$

In other words, $P(x)$ divides $G(x)$, as desired.

Note: Euclid's Lemma leads immediately to the fact that every polynomial over a field $\mathbb{F}$ has an essentially unique decomposition into irreducible (prime) factors.