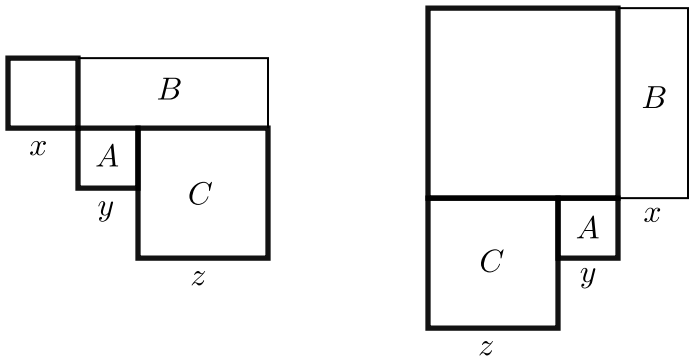
Math 461 **Spring 2020**
Homework 1 **Drew Armstrong**

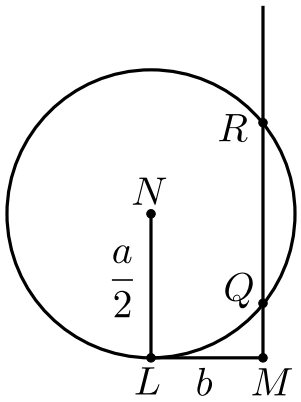
Problem 1. Al-Khwarizmi. If we do not accept negative numbers, then the hardest type quadratic equation comes down to the following geometric problem. In each diagram we have three squares and one rectangle. Assuming that the lengths satisfy $x + y = z$, prove that the areas satisfy $A + B = C$.



In either picture we observe that the rectangle has dimensions x and $y+z$, hence $B = x(y+z)$. By assumption we also have $A = y^2$, $C = z^2$ and $x + y = z$. It follows that

$$\begin{aligned} A + B &= y^2 + x(z + y) \\ &= y^2 + xz + xy \\ &= y(x + y) + xz \\ &= yz + xz \\ &= (x + y)z \\ &= z^2. \end{aligned}$$

Problem 2. Descartes. Consider the following figure from Descartes' *Geometry* (1637):



(a) Prove that the distances MQ and MR are solutions to the equation $y^2 + b^2 = ay$. [Hint: Let L be at the origin of the x, y-plane and use the equation of a circle.]
(b) Explain how the discriminant of the polynomial $y^2 - ay + b^2$ is related to the picture.

(a): It is possible to give a geometric proof by drawing two right triangles and then using the Pythagorean theorem. I will instead give an analytic proof. Let L be the origin $(0,0)$ in the x,y-plane, so that $M=(b,0)$ and $N=(0,a/2)$. The equation of the circle with center at $(0,a/2)$ and radius $a/2$ is

$$x^2+(y-a/2)^2=(a/2)^2.$$

And the equation of the vertical line is

$$x=b.$$

Combining these two equations gives

$$\begin{aligned} b^2+(y-a/2)^2&=(a/2)^2\\ b^2+y^2-ay+(a/2)^2&=(a/2)^2\\ b^2+y^2-ay&=0\\ b^2+y^2&=ay. \end{aligned}$$

In other words, the points of intersection of the line and circle are precisely the points (x,y) where $x=b$ and where y is a solution of the quadratic equation $b^2+y^2=ay$. According to the picture, the distances MQ and MR are the two solutions of this equation.

(b): But the quadratic formula tells us that

$$y=\frac{a\pm\sqrt{a^2-4b^2}}{2}=\frac{a}{2}\pm\frac{1}{2}\sqrt{a^2-4b^2}.$$

How does this relate to the picture? There are three cases:

- Note that $a^2-4b^2>0\Leftrightarrow|a/2|>|b|$. In this case the value of b is smaller than the radius of the circle, so the line intersects the circle in two points (as in the picture).
- Note that $a^2-4b^2=0\Leftrightarrow|a/2|=|b|$. In this case the line is tangent to the circle.
- Note that $a^2-4b^2<0\Leftrightarrow|a/2|<|b|$. In this case the line does not intersect the circle.

The algebra is smarter than the geometry because it can handle every case simultaneously, whereas the picture can only show one case. But the algebra also has some weird side-effects. For instance, if $|b|>|a/2|$ then it tells us that there are **two imaginary points of intersection** with coordinates

$$\left(b,\frac{a}{2}\pm\frac{1}{2}\sqrt{a^2-4b^2}\right)\quad\text{and}\quad\left(b,\frac{a}{2}\pm\frac{1}{2}\sqrt{a^2-4b^2}\right).$$

Problem 3. Uniqueness of Coefficients. Let $f(x)$ and $g(x)$ be polynomials with real coefficients and suppose that we have $f(\alpha)=g(\alpha)$ for all real numbers α. In this case prove that $f(x)$ and $g(x)$ have exactly the same coefficients. [Hint: Consider the polynomial $h(x)=f(x)-g(x)$. If $h(x)$ has at least one nonzero coefficient then we proved in class that the equation $h(x)=0$ has finitely many solutions.]

This is the most difficult problem. In order to make things clearer I will temporarily use the symbol $\equiv$ to denote the equality of formal polynomials. By definition we say that $f(x)\equiv g(x)$ when the two polynomials have exactly the same coefficients.

Proof. Let $\mathbb{F}$ be any **infinite field** (for example, $\mathbb{R}$) and let $f(x),g(x)\in\mathbb{F}[x]$ be two polynomials satisfying $f(\alpha)=g(\alpha)$ for all $\alpha\mathbb{F}$. (Here I use the symbol $=$ for equality of numbers.) Our goal is to show that $f(x)\equiv g(x)$ as formal polynomials.

To do this we define the polynomial $h(x) \equiv f(x) - g(x) \in \mathbb{F}[x]$. By assumption we have

$$h(\alpha) = f(\alpha) - g(\alpha) = 0 \quad \text{for all } \alpha \in \mathbb{F}.$$

Since the field is infinite this implies that the polynomial $h(x)$ has infinitely many roots. But we proved in class that any **nonzero** polynomial of degree n over a field has at most n roots in that field. It follows that $h(x) \equiv 0(x)$ must be the zero polynomial, and hence

$$\begin{aligned} f(x) - g(x) &\equiv h(x) \\ f(x) - g(x) &\equiv 0(x) \\ f(x) &\equiv g(x), \end{aligned}$$

as desired. □

Discussion: This problem might seem a bit silly, but it will become important later when we discuss finite fields. For example, we can regard the set $\mathbb{F}_2 = \{0, 1\}$ as a field by defining the operations

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Then we observe that the polynomials $f(x) = 1x + 1$ and $g(x) = 1x^2 + 0x + 1$ define the **same function**, even though they **do not have the same coefficients**:

α	0	1
$f(\alpha)$	1	0
$g(\alpha)$	1	0

Problem 4. Discriminant of a Quadratic. Suppose that the quadratic polynomial $f(x) = x^2 + px + q = 0$ can be factored as $x^2 + px + q = (x - r)(x - s)$ for some real numbers r and s.

(a) Use Problem 3 to show that $p = -r - s$ and $q = rs$.
(b) Show that $\text{Disc}(f) = (r - s)^2$.
(c) Show that $\text{Disc}(f) = 0$ if and only if $r = s$.

(a): I wasn't very clear in the statement of this problem, but let's assume that $x^2 + px + q \equiv (x - r)(x - s)$ as formal polynomials, so we do not have to invoke Problem 3. (Then this problem also works for finite fields.) Expanding the right hand side gives

$$\begin{aligned} x^2 + px + q &\equiv (x - r)(x - s) \\ x^2 + px + q &\equiv x^2 - (r + s)x + rs, \end{aligned}$$

and then comparing coefficients gives $p = -r - s$ and $q = rs$.

(b): The discriminant of $x^2 + px + q$ is defined to be $p^2 - 4q$. Then we observe that

$$p^2 - 4q = (-r - s)^2 - 4rs = r^2 + 2rs + s^2 - 4rs = r^2 - 2rs + s^2 = (r - s)^2.$$

(c): It follows from part (c) that

$$p^2 - 4q \quad \Leftrightarrow \quad (r - s)^2 \quad \Leftrightarrow \quad r = s.$$

Discussion: If $p, q \in \mathbb{R}$ then we are accustomed to saying that $x^2 + px + q = 0$ has one real solution in the case $p^2 - 4q = 0$ This problem suggests that it is more correct to say **two equal real solutions**, or **one real solution of multiplicity two**. From the modern point

of view we always say that a circle and a line meet in exactly two points; it's just that these two points might be identical or imaginary.

Problem 5. Factoring Cubic Polynomials. Factor each of the following cubic polynomials as $f(x) = (x-r)(x-s)(x-t)$ by first guessing a root, then using long division, and finally using the quadratic formula.

(a) $f(x) = x^3 - 2x^2 - 5x + 6$
(b) $f(x) = x^3 - 3x^2 + x + 1$
(c) $f(x) = x^3 - 1$

(a): We observe that $f(1) = 1$. Then we divide by $x - 1$ to obtain

$$\begin{array}{r|l} & x^2 - x - 6 \\ \hline x-1 & x^3 - 2x^2 - 5x + 6 \\ & -x^3 + x^2 \\ \hline & \quad -x^2 - 5x \\ & \quad x^2 - x \\ \hline & \quad\quad -6x + 6 \\ & \quad\quad 6x - 6 \\ \hline & \quad\quad\quad 0 \end{array}$$

It follows that $f(x) = (x-1)(x^2 - x - 6)$. The quadratic formula tells us that $x = -2$ and $x = 3$ are also roots, and we factor to obtain

$$f(x) = (x-1)(x+2)(x-3).$$

(b): We observe that $f(1) = 1$. Then we divide by $x - 1$ to obtain

$$\begin{array}{r|l} & x^2 - 2x - 1 \\ \hline x-1 & x^3 - 3x^2 + x + 1 \\ & -x^3 + x^2 \\ \hline & \quad -2x^2 + x \\ & \quad 2x^2 - 2x \\ \hline & \quad\quad -x + 1 \\ & \quad\quad x - 1 \\ \hline & \quad\quad\quad 0 \end{array}$$

It follows that $f(x) = (x-1)(x^2 - 2x - 1)$. Now the quadratic formula tells us that $x = (2 \pm \sqrt{2+4})/2 = 1 \pm \sqrt{2}$ and we factor to obtain

$$f(x) = (x-1)(x-1-\sqrt{2})(x-1+\sqrt{2}).$$

(b): We observe that $f(1) = 1$. Then we divide by $x - 1$ to obtain

$$\begin{array}{r|l} & x^2+x+1 \\ \hline x-1 & x^3 \quad\quad -1 \\ & -x^3+x^2 \\ \hline & \quad x^2 \\ & \quad -x^2+x \\ \hline & \quad\quad x-1 \\ & \quad\quad -x+1 \\ \hline & \quad\quad\quad 0 \end{array}$$

It follows that $f(x) = (x-1)(x^2+x+1)$. Now the quadratic formula tells us that $x = (1 \pm \sqrt{1-4})/2$ and we factor to obtain

$$f(x) = (x-1)\left(x - \frac{1+\sqrt{-3}}{2}\right)\left(x - \frac{1-\sqrt{-3}}{2}\right).$$

Discussion: The first polynomial splits over $\mathbb{Q}$, the second splits over $\mathbb{R}$ and the third splits over $\mathbb{C}$.

Problem 6. Alternate Proof of Descartes' Factor Theorem.

(a) For any variable x, constant a and positive integer n, show that

$$x^n - a^n = (x-a)(x^{n-1} + x^{n-2}a + \cdots + xa^{n-2} + a^{n-1}).$$

(b) For any polynomial $f(x)$ and constant a, use part (a) to show that

$$f(x) - f(a) = (x-a)g(x)$$

for some polynomial $g(x)$.

(a): I was a bit vague about the meaning of "variable" and "constant," but it doesn't matter. For any $n \geq 1$ we have

$$\begin{aligned} &(x-a)(x^{n-1} + x^{n-2}a + \cdots + xa^{n-2} + a^{n-1}) \\ &= \left[\begin{array}{cccccc} x(x^{n-1} & +x^{n-2}a & +\cdots & +a^{n-1}) & & \\ & -a(x^{n-1} & +\cdots & +xa^{n-2} & +a^{n-1}) & \end{array}\right] \\ &= \left[\begin{array}{cccccc} x^n & +x^{n-1}a & +\cdots & +xa^{n-1} & & \\ & -x^{n-1}a & -\cdots & -xa^{n-1} & -a^n & \end{array}\right] \\ &= x^n - a^n. \end{aligned}$$

(b): Let $f(x) = c_0 + c_1x + \cdots + c_nx^n$. In part (a) we proved that for any integer $k \geq 1$ we have $x^k - a^k = (x-a)q_k(x)$ for some specific polynomial $q_n(x)$. We conclude that

$$\begin{aligned} f(x) - f(a) &= \left[\begin{array}{ccccc} c_0 & +c_1x & +c_2x^2 & +\cdots & +c_nx^n \\ -c_0 & -c_1a & -c_2a^2 & +\cdots & -c_na^n \end{array}\right] \\ &= c_1(x-a) + c_2(x^2-a^2) + \cdots + c_n(x^n-a^n) \\ &= (x-a)\left[c_1q_1(x) + c_2q_2(x) + \cdots + c_nq_n(x)\right] \\ &= (x-a)g(x) \end{aligned}$$

for some specific polynomial $g(x)$.

Discussion: It follows from this that $f(a) = 0$ if and only if $f(x) = (x-a)g(x)$ for some specific polynomial $g(x)$.