Math 461 **Spring 2023**
Homework 1 **Drew Armstrong**

---

1. Roots vs Coefficients. One of the earliest theorems of algebra says that any symmetric function of the letters r_1 and r_2 can be written in terms of the *elementary symmetric functions* $e_1 = r_1 + r_2$ and $e_2 = r_1 r_2$. There is a general algorithm for many variables, but the case of two variables can done by trial-and-error.

(a) Express the symmetric function $(r_1 - r_2)^2$ in terms of e_1 and e_2.
(b) Express the symmetric function $r_1^2 + r_2^2$ in terms of e_1 and e_2.
(c) Expand the right hand side and compare coefficients to show that

$$x^2 - e_1 x + e_2 = (x - r_1)(x - r_2).$$

In other words, r_1, r_2 are the roots of the polynomial with coefficients $-e_1$ and e_2.[1]

(d) Let $x^2 + ax + b$ the the[2] polynomial with roots r_1^2 and r_2^2. Express a and b in terms of e_1 and e_2. [Hint: We must have $x^2 + ax + b = (x - r_1^2)(x - r_2^2)$. Expand the right hand side and compare coefficients.]

(a): We have

$$(r_1 - r_2)^2 = r_1^2 - 2r_1 r_2 + r_2^2 = (r_1 + r_2)^2 - 4r_1 r_2 = e_1^2 - 4e_2.$$

(a): We have

$$r_1^2 + r_2^2 = (r_1 + r_2)^2 - 2r_1 r_2 = e_1^2 - 2e_2.$$

(c): Since $e_1 = r_1 + r_2$ and $e_2 = r_1 r_2$ we have

$$(x - r_1)(x - r_2) = x^2 - (r_1 + r_2)x + r_1 r_2 = x^2 - e_1 x + e_2.$$

(d): We are given that $x^2 - e_1 x + e_2 = (x - r_1)(x - r_2)$. Now suppose that $x^2 + ax + b$ is the polynomial with roots r_1^2 and r_2, so that

$$\begin{aligned} x^2 + ax + b &= (x - r_1^2)(x - r_2^2) \\ &= x^2 - (r_1^2 + r_2^2)x + r_1^2 r_2^2. \end{aligned}$$

Since $r_1^2 + r_2^2 = e_1^2 - 2e_2$ (from part b) and $r_1^2 r_2^2 = (r_1 r_2)^2 = e_2^2$, we have

$$x^2 + ax + b = x^2 - (e_1^2 - 2e_2)x + e_2^2,$$

and comparing coefficients gives

$$\begin{cases} a &= -e_1^2 + 2e_2, \\ b &= e_2^2. \end{cases}$$

Example: Let $e_1 = 5$ and $e_2 = 6$ so that $x^2 - e_1 x + e_2$ has roots $r_1 = 2$ and $r_2 = 3$. Then the polynomial with roots $r_1^2 = 2^2 = 4$ and $r_2^2 = 3^2 = 9$ is, indeed,

$$x^2 - (e_1^2 - 2e_2)x + e_2^2 = x^2 - (5^2 - 2 \cdot 6)x + 6^2 = x^2 - 13x + 36.$$

---

[1] The negative sign in front of e_1 is just a convention.
[2] You can assume that the values of a and b are unique.

2. Integral Domains. Let $(R, +, \cdot, 0, 1)$ be a commutative ring. We say that R is an *integral domain* (or just a *domain*) when it satisfies the following property:

$$ab = 0 \implies a = 0 \text{ or } b = 0.$$

(a) *Cancellation.* Let $a, b, c \in R$ be elements of an integral domain. Prove that

$$ac = bc \text{ and } c \neq 0 \implies a = b.$$

(b) Prove that every field is an integral domain.

(c) Let R be an integral domain and consider the ring of polynomials $R[x]$. For any two nonzero polynomials $f(x), g(x) \in R[x]$, prove that

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

[Hint: Write $f(x) = \sum_k a_k x^k$, $g(x) = \sum_k b_k x^k$ and $f(x)g(x) = \sum_k c_k x^k$, so that $c_k = \sum_{i+j=k} a_i b_j$. Assume that $\deg(f) = m$ and $\deg(g) = n$ so that $a_m, b_n \neq 0$, $a_k = 0$ for all $k > m$ and $b_k = 0$ for all $k > n$. In this case prove that $c_{m+n} \neq 0$ and $c_k = 0$ for all $k > m + n$, hence $\deg(fg) = m + n = \deg(f) + \deg(g)$.]

(d) Let R be an integral domain. Use part (c) to prove that $R[x]$ is also an integral domain.

(a): Let R be an integral domain and consider $a, b, c \in R$. If $ac = bc$ and $c \neq 0$ then we have

$$\begin{aligned} ac &= bc \\ ac - bc &= 0 \\ (a - b)c &= 0 \\ a - b &= 0 \qquad\qquad \text{(because } R \text{ is a domain and } c \neq 0) \\ a &= b. \end{aligned}$$

(b): Let R be a field and consider $a, b \in R$. We want to show that $ab = 0$ implies $a = 0$ or $b = 0$. If $a = 0$ then we are done, so suppose that $a \neq 0$. Since R is a field this means that a^{-1} exists, so we get

$$\begin{aligned} ab &= 0 \\ a^{-1}ab &= a^{-1}0 \\ b &= 0. \end{aligned}$$

(c): There are two ways to do this.

Imprecise but Clear Proof. Let $\deg(f) = m$ and $\deg(g) = n$ so that

$$\begin{aligned} f(x) &= a_m x^m + \text{lower terms}, \\ g(x) &= b_n x^n + \text{lower terms}, \end{aligned}$$

where $a_m \neq 0$ and $b_n \neq 0$. Then the product is[3]

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

Since R is a domain, we know that $a_m \neq 0$ and $b_n \neq 0$ imply $a_m b_n \neq 0$, hence $f(x)g(x)$ has degree $m + n = \deg(f) + \deg(g)$ as desired. □

[3] But why? This is the imprecise part.

Precise but Annoying Proof. Let $\deg(f) = m$ and $\deg(g) = n$. By definition, this means we can write $f(x) = \sum a_k x^k$ and $g(x) = \sum_k b_k x^k$, with

$$a_m \neq 0, \quad b_n \neq 0, \quad a_k = 0 \text{ for all } k > m, \quad b_k = 0 \text{ for all } k > n.$$

Now consider the product $f(x)g(x)$ which is defined by

$$f(x)g(x) = \sum_{k \geq 0} c_k x^k, \quad \text{where} \quad c_k = \sum_{i+j=k} a_i b_j.$$

Our goal is to show that $c_{m+n} \neq 0$ and $c_k = 0$ for all $k > m+n$, so that

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

The key to the proof is to observe that $i+j > m+n$ implies $i > m$ or $j > n$.[4] If $k > m+n$ then I claim that every term $a_i b_j$ in the sum $c_k = \sum_{i+j=k} a_i b_j$ is zero. Indeed, if $i + j = k > m + n$ then we must have $i > m$ (in which case $a_i = 0$) or $j > n$ (in which case $b_j = 0$), and hence $a_i b_j = 0$. We have shown that $k > m + n$ implies $c_k = 0$.

Finally we will show that $c_{m+n} \neq 0$. To see this, I claim that every term $a_i b_j$ in the sum $c_{m+n} = \sum_{i+j=m+n} a_i b_j$ is zero, except for the single term $a_m b_n$, which is nonzero. Indeed, if $i + j = m + n$ then one of the following three cases must hold:[5]

- $i = m$ and $j = n$, in which case $a_m b_n \neq 0$ because $a_m \neq 0$ and $b_n \neq 0$,
- $i > m$, in which case $a_i = 0$ and hence $a_i b_j = 0$,
- $j > n$, in which case $b_j = 0$ and hence $a_i b_j = 0$.

Hence $c_{m+n} = a_m b_n \neq 0$. □

Remark: The first proof is clear to humans but a computer does not understand it. The second proof makes sense to computers but humans find it annoying. Sorry.

(d): Let R be a domain and consider any two nonzero polynomials $f(x), g(x) \in R[x]$. By part (c) we know that $\deg(fg) = \deg(f) + \deg(g) \geq 0 + 0 = 0$, which implies that $f(x)g(x)$ is not the zero polynomial.

Remark: Here I used the sort-of-weird but totally correct fact that

$$f(x) \neq 0 \quad \Longleftrightarrow \quad \deg(f) \geq 0.$$

Recall that $\deg(0) = -\infty$.

3. Uniqueness of Polynomial Remainders. Let R be a field[6] and consider the ring of polynomials $R[x]$. Consider two polynomials $f(x), g(x) \in R[x]$ with $g(x) \neq 0$ and suppose there exist polynomials $q_1(x), q_2(x), r_1(x), r_2(x) \in \mathbb{F}[x]$ satisfying

$$\begin{cases} f(x) = q_1(x)g(x) + r_1(x), \\ \deg(r_1) < \deg(g), \end{cases} \qquad \begin{cases} f(x) = q_2(x)g(x) + r_2(x), \\ \deg(r_2) < \deg(g). \end{cases}$$

In this case, prove that $r_1(x) = r_2(x)$ and $q_1(x) = q_2(x)$. [Hint: We have $g(x)[q_2(x) - q_1(x)] = r_1(x) - r_2(x)$, and you may assume that $\deg(r_1 - r_2) \leq \max\{\deg(r_1), \deg(r_2)\}$, so that $\deg(r_1 - r_2) < \deg(g)$. Now use Problem 2(c).]

[4] The contrapositive statement says that $i \leq m$ and $j \leq n$ imply $i + j \leq m + n$, which is true. To be completely pedantic, add j to both sides of $i \leq m$ to get $i + j \leq m + j$ then add m to both sides of $j \leq n$ to get $m + j \leq m + n$. Combine to get $i + j \leq m + j \leq m + n$.

[5] If none of these cases holds then we have $i \leq m$ and $j < n$ or $i < m$ and $j \leq n$, hence $i + j < m + n$.

[6] It suffices to let R be an integral domain.

Proof. Suppose we have polynomials f, g, q_1, q_2, r_1, r_2 satisfying the given hypotheses. Our goal is to show that $q_1 = q_2$ and $r_1 = r_2$. To do this, we first observe that

$$q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$$
$$g(x)\left[q_1(x) - q_2(x)\right] = r_2(x) - r_1(x).$$

Assume for contradiction that $r_1(x) \neq r_2(x)$, so that $r_2(x) - r_1(x) \neq 0$. Since R is a field (in particular, a domain) and $g(x) \neq 0$, the previous equation also tells us that $q_1(x) - q_2(x) \neq 0$. Thus we can take degrees and apply Problem 2(c) to get

$$\deg(g[q_1 - q_2]) = \deg(r_2 - r_1)$$
$$\deg(g) + \deg(q_1 - q_2) = \deg(r_2 - r_1).$$

On the one hand, this tells us that

$$\deg(r_2 - r_1) = \deg(g) + \deg(q_1 - q_2) \geq \deg(g).$$

On the other hand, since $\deg(r_1) < \deg(g)$ and $\deg(r_2) < \deg(g)$, we must have

$$\deg(r_2 - r_1) \leq \max\{\deg(r_1), \deg(r_2)\} < \deg(g).$$

This **contradiction** proves that $r_1(x) = r_2(x)$.

Finally, since $g(x)[q_1(x) - q_2(x)] = r_2(x) - r_1(x) = 0$ and $g(x) \neq 0$ (and since $R[x]$ is a domain) we conclude that $q_1(x) - q_2(x) = 0$ and hence $q_1(x) = q_2(x)$. $\square$

4. Same Function $\Longrightarrow$ Same Coefficients. Let R be a field with infinitely many elements, for example the real numbers $\mathbb{R}$.[7] Let $f(x), g(x) \in R[x]$ be any two monic polynomials satisfying $f(\alpha) = g(\alpha)$ for all $\alpha \in R$. In this case, prove that $f(x)$ and $g(x)$ must have the same coefficients. [Hint: Consider the polynomial $h(x) = f(x) - g(x)$. Descartes' Theorem implies that any (nonzero) polynomial of degree $n \geq 1$ over a field R has at most n distinct roots in that field.]

Proof. Let R be a field with infinitely many elements. Suppose that nonzero polynomials $f(x), g(x) \in R[x]$ satisfy $f(\alpha) = g(\alpha)$ for all $\alpha \in R$. In this case we will show that $f(x) = g(x)$, i.e., that f and g have the same coefficients.

The trick is to consider the polynomial $h(x) := f(x) - g(x)$. Then for all $\alpha \in R$ we have

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

Since R has infinitely many elements we observe that the polynomial $h(x) \in R[x]$ has infinitely many roots. But then Descartes' Factor Theorem implies that $h(x)$ is the zero polynomial, hence $f(x) = g(x)$. $\square$

Recall: Descartes' Factor Theorem implies that a **nonzero** polynomial $h(x) \in R[x]$ of degree $n \geq 0$ with coefficients in a field R has at most n distinct roots in R. If we find some polynomial $h(x)$ with infinitely many roots, then this implies that $h(x)$ must be the zero polynomial.

Remark: It was necessary to assume that R has infinitely many elements. For example, let R be the finite field with two elements: $R = \{0, 1\}$. Then the polynomials $f(x) = x + 1$ and $g(x) = x^2 + 1$ have the same values, but different coefficients.

[7] It suffices to let R be an integral domain with infinitely many elements, such as the integers $\mathbb{Z}$.

5. Alternate Proof of Descartes' Theorem.

(a) For any[8] variables x, y and for any integer $n \geq 2$, check[9] that

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-2} + y^{n-1}).$$

(b) Let R be any commutative ring. For any polynomial $f(x) \in R[x]$ and for any constant $\alpha \in R$, use part (a) to prove that

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

for some polynomial $g(x)$. [Hint: From part (a) we have $x^n - \alpha^n = (x-\alpha)h_{n-1}(x)$, with $h_{n-1}(x) = x^{n-1} + \alpha x^{n-2} + \cdots + \alpha^{n-2}x + \alpha^{n-1}$. Write $f(x) = \sum_k a_k x^k$ and observe that $f(x) - f(\alpha) = \sum_k a_k(x^k - \alpha^k)$.]

(a): When we expand the right hand side we observe that all but two terms cancel:

$$\begin{aligned}
&(x-y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}) \\
&= \begin{array}{l} x(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}) \\ -y(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}) \end{array} \\
&= \begin{array}{l} (x^n + \cancel{x^{n-1}y} + \cdots + \cancel{x^2y^{n-2}} + \cancel{xy^{n-1}}) \\ -(\cancel{x^{n-1}y} + \cancel{x^{n-2}y^2} + \cdots + \cancel{xy^{n-1}} + y^n) \end{array} \\
&= x^n - y^n.
\end{aligned}$$

(b): Let R be any commutative ring. Consider an integer $n \geq 1$ and a constant $\alpha \in R$. We know from part (a) that the polynomial $x^n - \alpha^n \in R[x]$ factors as

$$x^n - \alpha^n = (x-\alpha)(\text{some polynomial in } R[x]).$$

To simplify notation we will write $x^n - \alpha^n = (x-\alpha)h_{n-1}(x)$, where

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

Note that this polynomial $h_{n-1}(x) \in R[x]$ has degree $n-1$, hence the subscript.

Now consider an arbitrary polynomial $f(x) \in R[x]$, let's say

$$f(x) = a_n x^n + \cdots + a_1 x + a_0.$$

Then for any constant $\alpha \in R$ we have

$$\begin{aligned}
f(x) - f(\alpha) &= (a_n x^n + \cdots + a_1 x + \cancel{a_0}) - (a_n \alpha^n + \cdots + a_1 \alpha + \cancel{a_0}) \\
&= a_n(x^n - \alpha^n) + a_{n-1}(x^{n-1} - \alpha^{n-1}) + \cdots + a_1(x-\alpha) + 0 \\
&= a_n(x-\alpha)h_{n-1}(x) + a_{n-1}(x-\alpha)h_{n-2}(x) + \cdots + a_1(x-\alpha)h_0(x) \\
&= (x-\alpha)\left[a_n h_{n-1}(x) + a_{n-1}h_{n-2}(x) + \cdots + a_1 h_0(x)\right] \\
&= (x-\alpha)(\text{some polynomial in } R[x]).
\end{aligned}$$

□

[8] By convention we always assume that variables commute: $xy = yx$.

[9] When I say "check" there is usually not much to do. The goal is just to convince yourself and then write down how you would explain it to someone else.

Example: For $f(x) = 5x^3 - 2x^2 + 7$ we have

$$\begin{aligned}
f(x) - f(\alpha) &= (5x^3 - 2x^2 + 7) - (5\alpha^3 - 2\alpha^2 + 7) \\
&= 5(x^3 - \alpha^3) - 2(x^2 - \alpha^2) + 0(x - \alpha) + 0 \\
&= 5(x - \alpha)(x^2 + x\alpha + \alpha^2) - 2(x - \alpha)(x + \alpha) \\
&= (x - \alpha)\left[5(x^2 + x\alpha + \alpha^2) - 2(x + \alpha)\right].
\end{aligned}$$

Remark: This proof is more elementary than the one given in class, because it does not use the concept of quotient and remainder. Of course, that does not mean that this proof is "easier".