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.]

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:

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

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

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

(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.

3. Uniqueness of Polynomial Remainders. Let R be a field[3] and consider the ring of polynomials $R[x]$. Consider two polynomials $f(x), g(x) \in R[x]$ with $g(x) \not\equiv 0$ 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).]

---

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

4. Same Function $\implies$ Same Coefficients. Let R be a field with infinitely many elements, for example the real numbers $\mathbb{R}$.[4] 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.]

5. Alternate Proof of Descartes' Theorem.

(a) For any[5] variables x, y and for any integer $n \geq 2$, check[6] 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 $f(x) - f(\alpha) = \sum_k a_k(x^k - \alpha^k)$.]

---

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

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

[6] 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.