# Math 561/661 — Fall 2021
# Homework 2 — Drew Armstrong

**1. Cancellation in an Integral Domain.** A ring $(R,+,\cdot,0,1)$ is called an *integral domain* if it satisfies the following additional axiom:

(ID) For all $a,b\in R$, $ab=0$ implies that $a=0$ or $b=0$.

Important examples are the ring of integers $\mathbb{Z}$ and the ring of polynomials over a field $\mathbb{F}[x]$.

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

(b) If $R$ is an integral domain with $a,b,c\in R$, prove that

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

(c) Prove that a **finite** integral domain $R$ must be a field. [Hint: Given a nonzero element $c\in R$, consider the function $R\to R$ defined by $a\mapsto ac$. Use part (b) to show that this function is *injective* (one-to-one). Then use the finiteness of $R$ to show that this function is *surjective* (onto). Now what?]

**2. Uniqueness of Quotient and Remainder.** We proved in class that for any polynomials $f(x),g(x)\in\mathbb{F}[x]$ with $g(x)\neq 0$ there exist some polynomials $q(x),r(x)\in\mathbb{F}[x]$ satisfying[1]

$$\begin{cases} f(x)=g(x)q(x)+r(x),\\ \deg(r)<\deg(g).\end{cases}\tag{$*$}$$

In this problem you will show that the polynomials $q(x),r(x)$ are unique.

(a) For all polynomials $\phi(x),\mu(x)\in\mathbb{F}[x]$, show that $\deg(\phi\pm\mu)\leq\max\{\deg(\phi),\deg(\mu)\}$.

(b) Suppose that the pairs $q_1(x),r_1(x)$ and $q_2(x),r_2(x)$ both satisfy the properties $(*)$. Prove that we must have $r_1(x)=r_2(x)$. [Hint: We must have $[r_2(x)-r_1(x)]=g(x)[q_1(x)-q_2(x)]$. If $r_1(x)\neq r_2(x)$, show that the properties of degree, including part (a), lead to a contradiction.]

(c) Following from (b), use Problem 1(b) to conclude that $q_1(x)=q_2(x)$.

**3. Factorization of $x^n-1$ over $\mathbb{R}$.** For any integer $n\geq 1$, we proved in class that

$$x^n-1=(x-1)(x-\omega)(x-\omega^2)\cdots(x-\omega^{n-1}).$$

(a) Show that $\omega^k=\omega^{n-k}$ for all $k$ and use this to prove that

$$x^n-1=\begin{cases}(x-1)(x+1)\prod_{k=1}^{(n-2)/2}(x-\omega^k)(x-\omega^{-k}) & \text{if } n \text{ is even},\\ (x-1)\prod_{k=1}^{(n-1)/2}(x-\omega^k)(x-\omega^{-k}) & \text{if } n \text{ is odd.}\end{cases}$$

(b) Show that $\omega^{-k}=(\omega^k)^*$ and hence $\omega^k+\omega^{-k}=2\cos(2\pi k/n)$ for all $k$. Use this and part (b) to completely factor $x^n-1$ over the real numbers.

**4. The Regular Pentagon.** If $\omega=e^{2\pi i/5}$ then we know from Problem 3 that

$$x^5-1=(x-\omega^2)(x-\omega)(x-1)(x-\omega^{-1})(x-\omega^{-2}).$$

(a) Use this to show that $\omega^2+\omega+1+\omega^{-1}+\omega^{-2}=0$. [Hint: Compare coefficients.]

(b) Use part (a) and the fact that $z:=\omega+\omega^{-1}=2\cos(2\pi/5)$ to find an explicit formula for the number $\cos(2\pi/5)$. [Hint: Note that $z^2=(\omega+\omega^{-1})^2=\omega^2+2+\omega^{-2}$. Use this to show that $z$ satisfies a quadratic equation with real coefficients. Solve it.]

[1] The condition $\deg(r)<\deg(g)$ includes the possibility that $r(x)=0$.

(c) Combine parts (a) and (b) to obtain an expression for $\cos(4\pi/5)$. Then use Problem 4 to obtain the complete factorization of $x^5 - 1$ over the real numbers.

**5. The Splitting Field of $x^2 - 2$.** Consider the following set of real numbers:

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \subseteq \mathbb{R}.$$

One can check that this set is a subring[2] of $\mathbb{R}$. You can check this yourself if you want but it's pretty boring.

(a) For all $a, b, c, d \in \mathbb{Q}$, prove that

$$a + b\sqrt{2} = c + d\sqrt{2} \quad \Longleftrightarrow \quad a = c \text{ and } b = d.$$

(b) For all $a, b \in \mathbb{Q}$, prove that $a^2 - 2b^2 = 0$ if and only if $a + b\sqrt{2} = 0$. Use this result to prove that every nonzero element of $\mathbb{Q}(\sqrt{2})$ has a multiplicative inverse. [Hint: Rationalize the denominator.]

(c) Prove that $\sqrt{3}$ is not an element of $\mathbb{Q}(\sqrt{2})$, and hence that $\mathbb{Q}(\sqrt{2})$ is not equal to $\mathbb{R}$.

(d) Finally, suppose that $x^2 - 2$ splits over a field $\mathbb{E}$ where $\mathbb{Q} \subseteq \mathbb{E} \subseteq \mathbb{Q}(\sqrt{2})$. In this case, show that we must have $\mathbb{E} = \mathbb{Q}(\sqrt{2})$. [Hint: Suppose that $x^2 - 2 = (x - r_1)(x - r_2)$ for some $r_1, r_2 \in \mathbb{E}$. Now substitute $x = \sqrt{2}$.]

[Hint: You may assume that the real numbers $\sqrt{2}$ and $\sqrt{3}$ are not in $\mathbb{Q}$, i.e., they are irrational. More generally, for any positive integer $d \geq 1$ that is not a perfect square, the square roots of $d$ are irrational. You may have seen a proof of this result before. If not, you will see one later in this class.]

[2] If $(R, +, \cdot, 0, 1)$ is a ring, we say that a subset $S \subseteq R$ is a *subring* if $0, 1 \in S$ and if $a, b \in S$ implies that $a + b, ab \in S$.