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?]

(a): Suppose that $ac = bc$ for some elements $a, b, c \in R$ with $c \neq 0$. If R is a field then c has a multiplicative inverse $c^{-1} \in R$ and we obtain

$$\begin{aligned} ac &= bc \\ acc^{-1} &= bcc^{-1} \\ a &= b. \end{aligned}$$

(b): Suppose that $ac = bc$ for some elements $a, b, c \in R$ with $c \neq 0$. If R is an integral domain then we obtain

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

(c): Let $c \in R$ be a nonzero element of a finite integral domain. Consider the "multiplication by c" function $\mu_c := R \to R$ defined by $\mu_c(a) = ac$. Since R is a domain, we know from part (b) that $\mu_c(a) = \mu_c(b)$ implies $a = b$. In other words, μ_c is injective. Since R is finite this implies that

$$\#R = \#\{\mu_c(a) : a \in R\} = \#\{ac : a \in R\}.$$

Then since $\{ac : a \in R\}$ is a subset of R with the same size as R we must have

$$\{ac : a \in R\} = R.$$

Finally, since $1 \in \{ac : a \in R\}$ we have $ac = 1$ for some $a \in R$, which shows that c has a multiplicative inverse.

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]

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

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

---

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

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

(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 $[q_1(x) - q_2(x)] = g(x)[r_2(x) - r_1(x)]$. 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 to conclude that $q_1(x) = q_2(x)$.

(a): My goal for this problem was for you to observe that this is true, and for me to write a formal proof. I did not necessarily expect you to write a formal proof. Here it is.

If $\varphi(x) = 0$ or $\gamma(x) = 0$ then there is nothing to show. So let us suppose that $\deg(\varphi) = m \geq 0$ and $\deg(\gamma) = n \geq 0$. To specific, let $\varphi(x) = \sum_k a_k x^k$ and $\gamma(x) = \sum_k b_k x^k$ where $a_m, b_n \neq 0$ and $a_{m'}, b_{n'} = 0$ for all $m' > m$ and $n' > n$. If $r > \max\{m, n\}$ then we must have $r > m$ and $r > n$, which implies that the rth coefficient of $\varphi(x) \pm \gamma(x)$ is zero:

$$a_r \pm b_r = 0 \pm 0 = 0.$$

In other words, the degree of $\varphi(x) \pm \gamma(x)$ is $\leq \max\{\deg(\varphi), \deg(\gamma)\}$.

(b): Given $f(x), g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0$, let us suppose that

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

Comparing the two expressions for $f(x)$ gives

$$\begin{aligned} g(x)q_1(x) + r_1(x) &= g(x)q_2(x) + r_2(x) \\ g(x)\,[q_1(x) - q_2(x)] &= r_2(x) - r_1(x). \end{aligned}$$

Now let us assume for contradiction that $r_2(x) \neq r_1(x)$ and hence $r_2(x) - r_1(x) \neq 0$. Since $g(x) \neq 0$, the above equation and Problem 1(b) imply that $q_1(x) - q_2(x) \neq 0$. Then the additivity of degree gives

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

On the other hand, since $\deg(r_1) < \deg(g)$ and $\deg(r_2) < \deg(g)$, part (a) gives

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

which is a contradiction. Hence $r_1(x) = r_2(x)$.

(c): From part (b) we have

$$g(x)\,[q_1(x) - q_2(x)] = r_1(x) - r_2(x) = 0.$$

Since $g(x) \neq 0$, Problem 1(b) implies that $q_1(x) - q_2(x) = 0$ and hence $q_1(x) = q_2(x)$.

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.

(a): Let $\omega = e^{2\pi i/n}$, so that

$$\omega^n = (e^{2\pi i/n})^n = e^{2\pi i} = \cos(2\pi) + i\sin(2\pi) = 1.$$

Then for any integer $k \in \mathbb{Z}$ we have

$$\omega^{n-k} = \omega^n \omega^{-k} = 1\omega^{-k} = \omega^{-k}.$$

In particular, we can rewrite the nth roots of unity as follows:

$$\sqrt[n]{1} = \begin{cases} 1, \omega, \omega^{-1}, \omega^2, \omega^{-2}, \ldots, \omega^{(n-1)/2}, \omega^{-(n-1)/2} & \text{if } n \text{ is odd,} \\ 1, \omega, \omega^{-1}, \omega^2, \omega^{-2}, \ldots, \omega^{(n-2)/2}\omega^{-(n-2)/2}, -1 & \text{if } n \text{ is even.} \end{cases}$$

The desired factorizations follow.

(c): Since $|\omega|^2 = \cos^2(2\pi/n) + \sin^2(2\pi/n) = 1$ we have

$$\omega\omega^* = |\omega|^2 = 1,$$

which implies that $\omega^{-1} = \omega^* = \cos(2\pi/n) - i\sin(2\pi/n)$. Since $*$ preserves multiplication we have $(\alpha^*)^k = (\alpha^k)^*$ for all positive integers k. In particular, we have

$$\omega^{-k} = (\omega^{-1})^k = (\omega^*)^k = (\omega^k)^* = \cos(2\pi k/n) - i\sin(2\pi k/n),$$

which implies that

$$\begin{aligned} \omega^k + \omega^{-k} &= [\cos(2\pi k/n) + i\sin(2\pi k/n)] + [\cos(2\pi k/n) - i\sin(2\pi k/n)] \\ &= 2\cos(2\pi k/n), \end{aligned}$$

and hence

$$\begin{aligned} (x - \omega^k)(x - \omega^{-k}) &= x^2 - (\omega^k + \omega^{-k})x + \omega^k\omega^{-k} \\ &= x^2 - 2\cos(2\pi k/n)x + 1. \end{aligned}$$

Finally, we combine this with part (b) to obtain the complete factorization of $x^n - 1$ over the real numbers. When n is odd we get

$$x^n - 1 = (x-1)\prod_{k=1}^{(n-1)/2}(x^2 - 2\cos(2\pi k/n)x + 1),$$

and when n is even we get

$$x^n - 1 = (x-1)(x+1)\prod_{k=1}^{(n-2)/2}(x^2 - 2\cos(2\pi k/n)x + 1).$$

Remark: This factorization was first obtained by Roger Cotes in 1714, without the use of complex numbers. Cotes is known for preparing the second edition of Isaac Newton's *Principia*. Upon his early death in 1716 at the age of 33, Newton said: "If he had lived we would have known something."

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.]

(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.

(a): I will prove this for general n. There are three ways to do this. First we can expand the factorization of $x^n - 1$ to obtain

$$\begin{aligned} x^n - 1 &= (x-1)(x-\omega)\cdots(x-\omega^{n-1}) \\ x^n + 0x^{n-1} + \text{lower terms} &= x^n - (1+\omega+\cdots+\omega^{n-1})x^{n-1} + \text{lower terms}. \end{aligned}$$

Then comparing the coefficients of x^{n-1} gives

$$0 = 1 + \omega + \omega^2 + \cdots + \omega^{n-1}.$$

Second, we can use the factorization[2]

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

Substituting $x = \omega$ and using the facts that $\omega^n = 1$ and $\omega \neq 1$ gives

$$\begin{aligned} \omega^n - 1 &= (\omega - 1)(1 + \omega + \omega^2 + \cdots + \omega^{n-1}) \\ 0 &= (\omega - 1)(1 + \omega + \omega^2 + \cdots + \omega^{n-1}) \\ 0 &= 1 + \omega + \omega^2 + \cdots + \omega^{n-1}. \end{aligned}$$

Third, we can use geometry. Recall that the numbers $\omega^k = \cos(2\pi k/n) + i\sin(2\pi k/n)$ are the vertices of a regular n-gon in the complex plane, centered at the origin. Using the formula for the centroid of points in a vector space gives

$$\frac{1 + \omega + \omega^2 + \cdots + \omega^{n-1}}{n} = 0,$$

and the result follows.

In the case $n = 5$ we can rewrite the roots of unity to obtain

$$\omega^2 + \omega + 1 + \omega^{-1} + \omega^{-2} = \omega^2 + \omega + 1 + \omega^4 + \omega^3 = 0.$$

(b): Let $\omega = e^{2\pi i/5}$. From Problem 3(b) we know that

$$\omega^k + \omega^{-k} = 2\cos(2\pi k/5) \text{ for any integer } k \in \mathbb{Z}.$$

We will use this fact and part (a) to obtain an explicit formula for $\cos(2\pi/5)$. First we write $z = \omega + \omega^{-1} = 2\cos(2\pi/5)$ and observe that

$$z^2 = (\omega + \omega^{-1}) = \omega^2 + 2\omega\omega^{-1} + \omega^{-2} = \omega^2 + 2 + \omega^{-2}.$$

It follows that

$$\begin{aligned} z^2 + z &= (\omega^2 + 2 + \omega^{-2}) + (\omega + \omega^{-1}) \\ &= (\omega^2 + \omega + 1 + \omega^{-1} + \omega^{-2}) + 1 \\ &= 0 + 1 \\ &= 1. \end{aligned}$$

[2]This factorization can be easily checked. You may have used it in calculus to prove that $1 + x + x^2 + \cdots = 1/(1-x)$ when $|x| < 1$. To see this, use the fact that $x^n \to 0$ as $n \to \infty$.

Solving the quadratic equation $z^2 + z - 1$ gives

$$2\cos(2\pi/5) = z = \frac{-1 \pm \sqrt{5}}{2},$$

Since $\cos(2\pi/5) > 0$ we choose the plus sign to obtain

$$\cos\left(\frac{2\pi}{5}\right) = \frac{-1+\sqrt{5}}{4}.$$

(c): To obtain a formula for $\cos(4\pi/5)$ we use parts (b) and 3(b) see that[3]

$$\begin{aligned} \omega^2 + \omega + 1 + \omega^{-1} + \omega^{-2} &= 0 \\ \omega^2 + \omega^{-2} &= -1 - (\omega + \omega^{-1}) \\ 2\cos(4\pi/5) &= -1 - 2\cos(2\pi/5) \\ 2\cos(4\pi/5) &= -1 - (-1+\sqrt{5})/2 \\ 2\cos(4\pi/5) &= (-1-\sqrt{5})/2 \\ \cos\left(\frac{4\pi}{5}\right) &= \frac{-1-\sqrt{5}}{4}. \end{aligned}$$

The following formulas are also true:[4]

$$\cos\left(\frac{2\pi}{5}\right) = \frac{\sqrt{3-\sqrt{5}}}{2\sqrt{2}} \quad \text{and} \quad \cos\left(\frac{4\pi}{5}\right) = -\frac{\sqrt{3+\sqrt{5}}}{2\sqrt{2}},$$

But I don't like these so much because of the nested square roots.

Finally, by combining our formulas for $\cos(2\pi/5)$ and $\cos(4\pi/5)$ we obtain an explicit factorization for $x^5 - 1$ in terms of polynomials with real coefficients:

$$\begin{aligned} x^5 - 1 &= (x-1)\left[(x-\omega)(x-\omega^{-1})\right]\left[(x-\omega^2)(x-\omega^{-2})\right] \\ &= (x-1)(x^2 - 2\cos(2\pi/5)x + 1)(x^2 - 2\cos(4\pi/5)x + 1) \\ &= (x-1)\left(x^2 - \frac{-1+\sqrt{5}}{2}x + 1\right)\left(x^2 - \frac{-1-\sqrt{5}}{2}x + 1\right) \\ &= (x-1)\left(x^2 + \frac{1-\sqrt{5}}{2}x + 1\right)\left(x^2 + \frac{1+\sqrt{5}}{2}x + 1\right) \end{aligned}$$

Imagine trying to find this factorization without using complex 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[5] of $\mathbb{R}$. You can check this yourself if you want but it's pretty boring.

---

[3]Alternatively, you could define $u = \omega^2 + \omega^{-2} = 2\cos(4\pi/5)$ and check that the same equation holds: $u^2 + u - 1 = 0$. Thus $2\cos(4\pi/5)$ is the other root of the quadratic equation from part (a).

[4]This formula for $\cos(2\pi/5)$ can be found by writing the equation $z^2 + z - 1$ as $z = \sqrt{1-z}$.

[5]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 $a + b, ab \in S$.

(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.]

(a): If $a = c$ and $b = d$ then clearly $a + b\sqrt{2} = c + d\sqrt{2}$. Conversely, suppose that $a + b\sqrt{2} = c + d\sqrt{2}$ for some $a, b, c, d \in \mathbb{Q}$. If $b = d$ then we also have $a = c$, so let us assume for contradiction that $b \neq d$. Then we get

$$\begin{aligned} a + b\sqrt{2} &= c + d\sqrt{2} \\ \sqrt{2} &= (a - c)/(d - b), \end{aligned}$$

which contradicts the fact that $\sqrt{2}$ is irrational.

Remark: We have just proved that $\mathbb{Q}(\sqrt{2})$ is a **two-dimensional vector space over** $\mathbb{Q}$ with standard basis $1, \sqrt{2}$.

(b): If $a + b\sqrt{2} = 0$ then we have $a = -b\sqrt{2}$ and squaring both sides gives $a^2 = 2b^2$, hence $a^2 - 2b^2 = 0$. Conversely, suppose that we have $a^2 - 2b^2 = 0$ for some $a, b \in \mathbb{Q}$. If $b = 0$ then we also have $a = 0$, and hence $a + b\sqrt{2} = 0$. So let us assume for contradiction that $b \neq 0$. Then we get

$$\begin{aligned} a^2 - 2b^2 &= 0 \\ a^2 &= 2b^2 \\ (a/b)^2 &= 2, \end{aligned}$$

which contradicts the fact that $\sqrt{2}$ is irrational.

It follows that for any $a, b \in \mathbb{Q}$ with $a + b\sqrt{2} \neq 0$ we can write[6]

$$\begin{aligned} \frac{1}{a + b\sqrt{2}} &= \frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} \\ &= \frac{a - b\sqrt{2}}{a^2 - 2b^2} \\ &= \left(\frac{a}{a^2 - 2b^2}\right) + \left(\frac{-b}{a^2 - 2b^2}\right)\sqrt{2}, \end{aligned}$$

where $a/(a^2 - 2b^2)$ and $-b/(a^2 - 2b^2)$ are rational numbers.

[6] Technically speaking, this derivation uses the fact that $a - b\sqrt{2} \neq 0$. This can be shown by observing that $(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$ and $a^2 - 2b^2 \neq 0$.

(c): Suppose for contradiction that $\sqrt{3} = a + b\sqrt{2}$ for some $a, b \in \mathbb{Q}$. If $b = 0$ then we obtain $\sqrt{3} = a$, which contradicts the fact that $\sqrt{3}$ is irrational. So let us suppose that $b \neq 0$. If $a = 0$ then we have

$$\begin{aligned}
\sqrt{3} &= b\sqrt{2} \\
\sqrt{3}\sqrt{2} &= 2b \\
\sqrt{6} &= 2b,
\end{aligned}$$

which contradicts the fact that $\sqrt{6}$ is irrational. [Oops, I should have told you to assume this as well.] Finally, if $b \neq 0$ and $a \neq 0$ then we have $2ab \neq 0$ and hence

$$\begin{aligned}
\sqrt{3} &= a + b\sqrt{2} \\
3 &= (a + b\sqrt{2})^2 \\
3 &= a^2 + 2b^2 + 2ab\sqrt{2} \\
\frac{3 - a^2 - 2b^2}{2ab} &= \sqrt{2},
\end{aligned}$$

which contradicts the fact that $\sqrt{2}$ is irrational.

Remark: Wow, that was tricky. And we still haven't proved that $\sqrt{2}, \sqrt{3}, \sqrt{6}$ are irrational. This will be much easier to do once we have discussed unique prime factorization.

(d): We have seen that $\mathbb{Q}(\sqrt{2})$ is a proper subfield of $\mathbb{R}$ over which the polynomial $x^2 - 2$ splits. I claim that $\mathbb{Q}(\sqrt{2})$ is the splitting field. To see this, consider any field $\mathbb{Q} \subseteq \mathbb{E} \subseteq \mathbb{Q}(\sqrt{2})$ and suppose that $x^2 - 2$ splits over $\mathbb{E}$. In other words, suppose that we have $x^2 - 2 = (x - r_1)(x - r_2)$ for some $r_1, r_2 \in \mathbb{E}$. Then substituting $x = \sqrt{2}$ gives

$$(\sqrt{2} - r_1)(\sqrt{2} - r_2) = (\sqrt{2})^2 - 2 = 0,$$

which implies that $r_1 = \sqrt{2}$ or $r_2 = \sqrt{2}$. In either case, we find that $\sqrt{2} \in \mathbb{E}$. Finally, we conclude that $\mathbb{E} = \mathbb{Q}(\sqrt{2})$ since for any $a, b \in \mathbb{Q}$ we have $a, b, \sqrt{2} \in \mathbb{E}$ and hence $a + b\sqrt{2} \in \mathbb{E}$.

Remark: It will turn out later that the solvability of a polynomial in terms of radicals is related to the symmetries of its splitting field. A symmetry of a field extension $\mathbb{E} \supseteq \mathbb{F}$ is an invertible function $\sigma : \mathbb{E} \to \mathbb{E}$ satisfying

- $\sigma(a) = a$ for all $a \in \mathbb{F}$,
- $\sigma(a + b) = \sigma(a) + \sigma(b)$ for all $a, b \in \mathbb{E}$,
- $\sigma(ab) = \sigma(a)\sigma(b)$ for all $a, b \in \mathbb{E}$.

For example, complex conjugation is a symmetry of the field extension $\mathbb{C} \supseteq \mathbb{R}$ and the map $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is a symmetry of the field extension $\mathbb{Q}(\sqrt{2}) \supseteq \mathbb{Q}$.