Math 461 **Spring 2020**
Homework 3 **Drew Armstrong**

Problem 1. Difference of nth Powers. Let $n \geq 1$ be a positive integer and let $\omega = e^{2\pi i/n}$. Prove that for all complex numbers $\alpha, \beta \in \mathbb{C}$ we have

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

Recall that the polynomial $x^n - 1 \in \mathbb{C}[x]$ splits as follows:

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

Now consider any complex numbers $\alpha, \beta \in \mathbb{C}$. If $\beta = 0$ then there is nothing to show, so we may assume that $\beta \neq 0$. Then we evaluate the polynomial $x^n - 1$ at $x = \alpha/\beta$ to obtain

$$\begin{aligned}
(\alpha/\beta)^n - 1 &= (\alpha/\beta - 1)(\alpha/\beta - \omega)(\alpha/\beta - \omega^2)\cdots(\alpha/\beta - \omega^{n-1}) \\
\beta^n\left[(\alpha/\beta)^n - 1\right] &= \beta^n\left[(\alpha/\beta - 1)(\alpha/\beta - \omega)(\alpha/\beta - \omega^2)\cdots(\alpha/\beta - \omega^{n-1})\right] \\
\alpha^n - \beta^n &= \left[\beta(\alpha/\beta - 1)\right]\left[\beta(\alpha/\beta - \omega)\right]\left[\beta(\alpha/\beta - \omega^2)\right]\cdots\left[\beta(\alpha/\beta - \omega^{n-1})\right] \\
&= (\alpha - \beta)(\alpha - \omega\beta)(\alpha - \omega^2\beta)\cdots(\alpha - \omega^{n-1}\beta).
\end{aligned}$$

Problem 2. Integral Domains. We say that a (commutative) ring R is an *integral domain* if for all $a, b \in R$ we have

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

The prototypical example is the ring of integers $\mathbb{Z}$, hence the name.

(a) Prove that a field is an integral domain.
(b) If R is integral domain, prove that $R[x]$ is integral domain. [Hint: Leading coefficients.]
(c) If $a, b, c \in R$ and $a \neq 0$ in an integral domain, prove that $ab = ac$ implies $b = c$.
(d) Consider any $a, b \in R$ with $a|b$ and $b|a$. In this case, use part (c) to show that $a = ub$ for some **invertible** element $u \in R$ (called a *unit*).

(a): Let $\mathbb{F}$ be a field and consider $a, b \in \mathbb{F}$ with $ab = 0$. If $a = 0$ then we are done. Otherwise, if $a \neq 0$ then since $\mathbb{F}$ is a field we can multiply both sides of $ab = 0$ by a^{-1} to obtain $b = 0a^{-1} = 0$.

(b): Let R be an integral domain and consider two nonzero polynomials $f(x), g(x) \in R[x]$. By definition, this means that

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

for some non-negative integers $0 \leq m, n \in \mathbb{Z}$ and nonzero ring elements $0 \neq a_m, b_n \in R$. By multiplying $f(x)$ and $g(x)$ we obtain

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

Finally, since R is an integral domain we know that $a_m b_n \neq 0$, which implies that $f(x)g(x)$ is not the zero polynomial.

(c): Let R be an integral domain and consider any $a, b, c \in R$ satisfying $ab = ac$ and $a \neq 0$. By rearranging the equation $ab = ac$ we have

$$\begin{aligned}
ab &= ac \\
ab - ac &= 0 \\
a(b - c) &= 0.
\end{aligned}$$

Then since $a \neq 0$ we conclude that $b - c = 0$, hence $b = c$. [Remark: We are not allowed to "divide both sides by a" because R is not necessarily a field.]

(d): Let R be an integral domain and consider any $a, b \in R$ with $a|b$ and $b|a$. (We will assume that a and b are both nonzero.) By definition this means that $a = ub$ and $b = va$ for some elements $u, v \in R$. In order to show that u is invertible, we observe that $a = ub = uva$ and then we cancel a from both sides to obtain $1 = uv$.

Discussion: Every field is an integral domain but not every integral domain is a field. For example, the rings $\mathbb{Z}$ and $\mathbb{F}[x]$ are integral domains but they are not fields (for example, because $1/2$ is not an integer and $1/x$ is not a polynomial). Later in the course we will encounter rings that are **not** integral domains. For example, let $\mathbb{Z}/4\mathbb{Z}$ denote the set $\{0, 1, 2, 3\}$ together with the following operations:

$$\begin{array}{c|cccc} + & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 1 & 2 & 3 & 0 \\ 2 & 2 & 3 & 0 & 1 \\ 3 & 3 & 0 & 1 & 2 \end{array} \qquad \begin{array}{c|cccc} \times & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & 3 \\ 2 & 0 & 2 & 0 & 2 \\ 3 & 0 & 3 & 2 & 1 \end{array}$$

We will see that these operations define a ring structure on the set $\{0, 1, 2, 3\}$. However, this ring is not an integral domain because $2 \cdot 2 = 0$.

Problem 3. Bézout's Identity. Let $a, b \in \mathbb{Z}$ (not both zero) and consider the set

$$S = \{ax + by : x, y \in \mathbb{Z}, ax + by \geq 1\}.$$

By well-ordering this set contains a smallest elemement; call it $d \in S$.

(a) Prove that $d|a$ and $d|b$. [Hint: There exist $q, r \in \mathbb{Z}$ with $a = dq + r$ and $0 \leq r < d$. Show that $r \geq 1$ leads to a contradiction.]

(b) If $e|a$ and $e|b$ for some $e \in \mathbb{Z}$, show that $e|d$.

It follows that d is the *greatest common divisor* of a and b. In particular, we have shown that there exist some (non-unique) integers $x, y \in \mathbb{Z}$ satisfying $\gcd(a, b) = ax + by$.

(a): Since $d \in S$ there exist some $x, y \in \mathbb{Z}$ satisfying $d = ax + by \geq 1$. Then from the Division Theorem there exist some $q, r \in \mathbb{Z}$ with $a = dq + r$ and $0 \leq r < d$. Observe that

$$d > r = a - dq = a - (ax + by)q = a(1 - xq) + b(-yq) = ax' + by' \geq 0$$

for some $x', y' \in \mathbb{Z}$. If $r \neq 0$ then this implies that r is an element of S that is strictly smaller than d, which is a contradiction. Therefore we must have $r = 0$ and hence $d|a$. A similar argument shows that $d|b$.

(b): Let $e \in \mathbb{Z}$ be any integer satisfying $e|a$ and $e|b$. Let's say $a = ea'$ and $b = eb'$ for some $a', b' \in \mathbb{Z}$. Then since $d = ax + by$ for some $x, y \in \mathbb{Z}$ we have

$$d = ax + by = ea'x + eb'y = e(a'x + b'y),$$

and hence $e|d$.

In summary, we have shown that $d = ax + by$ is a common divisor of a and b, which is larger than (in fact, divisible by) every other common divisor. In other words, $d = \gcd(a, b)$.

Problem 4. De Moivre's Formula.

(a) Use de Moivre's formula to express $\cos(2\theta)$ as a polynomial in $\cos\theta$.

(b) Solve this polynomial to obtain a formula for $\cos\theta$ in terms of $\cos(2\theta)$.

(c) Use your formula from (b) to obtain exact values for $\cos(\pi/2^n)$ when $n = 1, 2, 3, 4$.

(a): De Moivre's formula says that

$$\begin{aligned}\cos(2\theta) + i\sin(2\theta) &= (\cos\theta + i\sin\theta)^2 \\ &= (\cos^2\theta - \sin^2\theta) + i(2\cos\theta\sin\theta).\end{aligned}$$

Then comparing real parts gives

$$\cos(2\theta) = \cos^2\theta - \sin^2\theta = \cos^2\theta - (1 - \cos^2\theta) = 2\cos^2\theta - 1.$$

(b): Rearranging gives

$$2(\cos\theta)^2 + 0(\cos\theta) + (-1 - \cos(2\theta)) = 0,$$

hence the quadratic formula says

$$\cos\theta = \frac{0 \pm \sqrt{4(1 + \cos(2\theta))}}{4} = \pm\frac{1}{2}\sqrt{2 + 2\cos(2\theta)}.$$

If $-\pi/2 \leq \theta \leq \pi/2$ then we choose the positive sign; otherwise we choose the negative sign.

(c): Since $\cos(\pi/2) = 0$, the formula from part (b) gives

$$\cos(\pi/4) = \frac{1}{2}\sqrt{2 + 2\cos(\pi/2)} = \frac{1}{2}\sqrt{2}.$$

Applying the formula again gives

$$\cos(\pi/8) = \frac{1}{2}\sqrt{2 + 2\cos(\pi/4)} = \frac{1}{2}\sqrt{2 + \sqrt{2}},$$

and again gives

$$\cos(\pi/16) = \frac{1}{2}\sqrt{2 + 2\cos(\pi/8)} = \frac{1}{2}\sqrt{2 + \sqrt{2 + \sqrt{2}}}.$$

Discussion: Since $\cos(\pi/2^n) \to 1$ as $n \to \infty$, we conclude that

$$1 = \frac{1}{2}\sqrt{2 + \sqrt{2 + \sqrt{2 + \sqrt{2 + \cdots}}}}.$$

That's strange.

Problem 5. Quadratic Formula Again.

(a) Find the two complex square roots of i. [Hint: Express i in polar form.]
(b) Use part (a) and the quadratic formula to solve the following equation for x:

$$x^2 + (2i)x - (1 + i) = 0.$$

(a): For any angle $\theta \in \mathbb{R}$, the square roots of $e^{i\theta}$ are $e^{i\theta/2}$ and $e^{i(\theta/2+\pi)} = -e^{i\theta/2}$. Since $i = e^{i\pi/2}$ this implies that the square roots of i are $e^{i\pi/4} = (1 + i)/\sqrt{2}$ and $e^{i5\pi/4} = -(1 + i)/\sqrt{2}$, which we can express in Cartesian form as

$$\begin{aligned}e^{i\pi/4} &= \cos(\pi/4) + i\sin(\pi/4) = 1/\sqrt{2} + i/\sqrt{2} = (1 + i)/\sqrt{2}, \\ e^{i5\pi/4} &= \cos(5\pi/4) + i\sin(5\pi/4) = -1/\sqrt{2} - i/\sqrt{2} = -(1 + i)/\sqrt{2}.\end{aligned}$$

(b): Applying the quadratic formula to the equation $x^2 + (2i)x - (1+i) = 0$ gives

$$x = \frac{-2i \pm \sqrt{(2i)^2 + 4(1+i)}}{2} = \frac{-2i \pm \sqrt{(-4+4+i)}}{2} = \frac{-2i \pm 2\sqrt{i}}{2} = -i \pm \sqrt{i}$$

Then combining this with the result of (a) gives

$$x = -i \pm \sqrt{i} = -i \pm (1+i)/\sqrt{2}$$

Note that these roots are not complex conjugates, reflecting the fact that the polynomial does not have real coefficients.

Problem 6. Cyclotomic Polynomials. Let $e^{2\pi i/n}$ for some positive integer $n \geq 1$ and recall that $\omega^1, \omega^2, \ldots, \omega^n$ are the nth roots of unity. We say that ω^k is a *primitive nth root of unity* when $\gcd(k,n) = 1$, and we define the *nth cyclotomic polynomial* as follows:

$$\Phi_n(x) := \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} (x - \omega^k).$$

(a) Compute the polynomials $\Phi_1(x)$, $\Phi_2(x)$, $\Phi_4(x)$, $\Phi_8(x)$, and observe that each has integer coefficients. [Hint: Problem 5(a).]

(b) Prove that the polynomial $x^8 - 1 \in \mathbb{Q}[x]$ can be factored as follows:

$$x^8 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_8(x).$$

(a): We will use the notation $\omega_d = e^{2\pi i/d}$ to distinguish the dth roots of unity for different values of d. The primitive 1st roots of unity are $\omega_1^1 = 1$, hence

$$\Phi_1(x) = (x - \omega_1^1) = x - 1.$$

The primitive 2nd roots of unity are $\omega_2^1 = -1$, hence

$$\Phi_2(x) = (x - \omega_2^1) = x + 1.$$

The primitive 4th roots of unity are $\omega_4^1 = i$ and $\omega_4^3 = -i$, hence

$$\Phi_2(x) = (x - \omega_4^1)(x - \omega_4^3) = (x - i)(x + i) = x^2 + 1.$$

Finally, the primitive 8th roots of unity are $\omega_8^1, \omega_8^3, \omega_8^5, \omega_8^7$. To be explicit, the formulas for $\cos(2\pi k/8)$ and $\sin(2\pi k/8)$ tell us that

$$\begin{aligned}
\omega_8^1 &= \cos(2\pi/8) + i\sin(2\pi/8) = (1+i)/\sqrt{2}, \\
\omega_8^3 &= \cos(6\pi/8) + i\sin(6\pi/8) = (-1+i)/\sqrt{2}, \\
\omega_8^5 &= \cos(10\pi/8) + i\sin(10\pi/8) = (-1-i)/\sqrt{2}, \\
\omega_8^7 &= \cos(14\pi/8) + i\sin(14\pi/8) = (1-i)/\sqrt{2}.
\end{aligned}$$

By grouping these into complex conjugate pairs, we obtain

$$\begin{aligned}
\Phi_8(x) &= (x - (1+i)/\sqrt{2})(x - (1-i)/\sqrt{2})(x - (-1+i)/\sqrt{2})(x - (-1-i)/\sqrt{2}) \\
&= (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1) \\
&= x^4 + 1.
\end{aligned}$$

Alternatively, one could prove that the **primitive** 8th roots of $+1$ are **all** of the 4th roots of -1. Then it is clear that $\Phi_8(x) = x^4 - (-1)$.

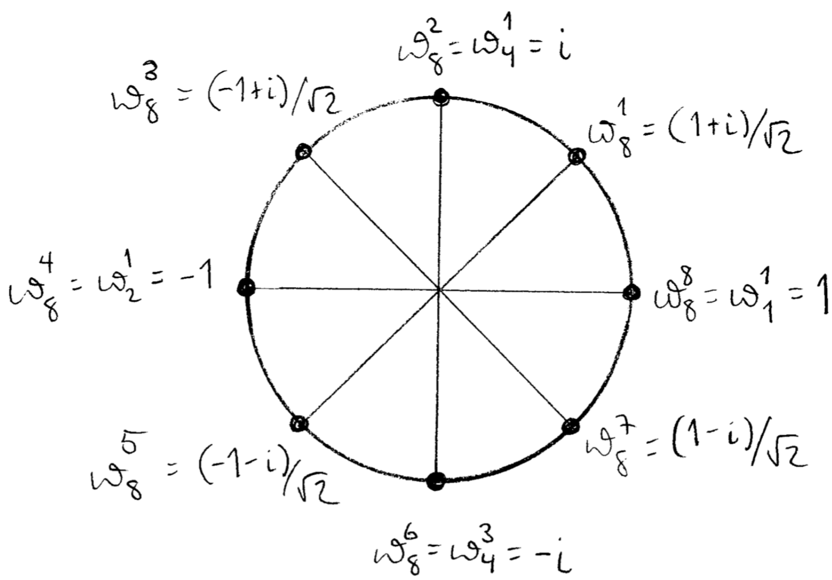
(b): One can check by hand that

$$\Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_8(x) = (x-1)(x+1)(x^2+1)(x^4+1) = x^8 - 1.$$

Alternatively, one can use the fact that $\omega_b^a = e^{2\pi i a/b} = e^{2\pi i c/d} = \omega_d^c$ for all fractions satisfying $a/b = c/d$. By reducing the fractions $k/8$ $(1 \le k \le 8)$ into lowest terms, we observe that the 8th roots of unity can be partitioned into the sets of **primitive** dth roots of unity for each divisor $d = \{1, 2, 4, 8\}$ of 8:

$$\begin{aligned}
&\{\omega_8^1, \omega_8^2, \omega_8^3, \omega_8^4, \omega_8^5, \omega_8^6, \omega_8^7, \omega_8^8\} \\
&= \{\omega_8^1, \omega_4^1, \omega_8^3, \omega_2^1, \omega_8^5, \omega_4^3, \omega_8^7, \omega_1^1\} \\
&= \{\omega_1^1\} \cup \{\omega_2^1\} \cup \{\omega_4^1, \omega_4^3\} \cup \{\omega_8^1, \omega_8^3, \omega_8^5, \omega_8^7\}.
\end{aligned}$$

Then we obtain the factorization $x^8 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_8(x)$ without even knowing the coefficients of the cyclotomic polynomials. Here is a picture:



Discussion: This same argument can be used to prove the identity

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

for any $n \ge 1$. I might ask you to prove this on a future homework. I might also ask you to use this identity to prove by induction that $\Phi_n(x)$ always has integer coefficients.