Problem 1 (13.6.6). Prove that for n odd, $n > 1$, $\Phi_{2n}(x) = \Phi_n(-x)$.

Proof. First note that for any polynomial that $f(x)f(-x) = f(x^2)$. Applying this to our cyclotomic polynomial we get that

$$\Phi_n(x)\Phi_n(-x) = \Phi_n(x^2)$$

Moreover this implies that

$$\Phi_n(-x) = \frac{\Phi_n(x^2)}{\Phi_n(x)}$$

If we look at the expansion of $\Phi_n(x^2)$ we have

$$\Phi_n(x^2) = \prod_{1\leq d<n,\ (d,n)=1} (x^2 - \zeta_n^d)$$

We can factor to get

$$\Phi_n(x^2) = \prod_{1\leq d<n,\ (d,n)=1} (x - \zeta_n^{d/2})(x + \zeta_n^{d/2})$$

Applying the fact that for roots of unity that $\zeta_n^d = -\zeta_n^{n/2+d}$ we get

$$\Phi_n(x^2) = \prod_{1\leq d<n,\ (d,n)=1} (x - \zeta_n^{d/2})(x - \zeta_n^{(n+d)/2})$$

Then by changing the indexes we get

$$\Phi_n(x^2) = \prod_{1\leq d<n,\ (d,n)=1} (x - \zeta_{2n}^{d})(x - \zeta_{2n}^{n+d})$$

Returning to our quotient we now have

$$\frac{\Phi_n(x^2)}{\Phi_n(x)} = \prod_{1\leq d<n,\ (d,n)=1} \frac{(x - \zeta_{2n}^{d})(x - \zeta_{2n}^{n+d})}{(x - \zeta_n^d)}$$

Since n is odd and greater than 1 we have that if $\gcd(d, n) = 1$ then either $\gcd(d, 2n) = 1$ or $\gcd(d + n, 2n) = 1$. Also note that $\varphi(2n) = \varphi(2)\varphi(n) = \varphi(n)$ implying that $2n$ and n have the same number of numbers that are relatively prime that are smaller than them. Thus all of the necessary terms for $\Phi_{2n}(x)$ appear in the earlier quotient.

If $\gcd(d, 2n) = 1$ or $\gcd(d + n, 2n) = 1$ this implies that the other is even as n is odd. Let $2k$ be the even number among d or $d + n$. Then we can rewrite the prior expression as

$$\frac{\Phi_n(x^2)}{\Phi_n(x)} = \Phi_{2n}(x) \prod_{1\leq d<n,\ (d,n)=1} \frac{(x - \zeta_n^k)}{(x - \zeta_n^d)}$$

However the product on the right is equal to 1 **(justify better)** as each k above will either directly match a d or $n/2$ factor will wrap it to around. Thus giving us the equality

$$\Phi_n(-x) = \frac{\Phi_n(x^2)}{\Phi_n(x)} = \Phi_{2n}(x)$$

Therefore if n is odd and $n > 1$ we have that $\Phi_{2n}(x) = \Phi_n(-x)$. □

Problem 2 (13.6.9). Suppose A is an $n \times n$ matrix over $\mathbb{C}$ for which $A^k = I$ for some integer $k \geq 1$. Show that A can be diagonalized. Show that the matrix $A = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ where α is an element of a field of characteristic p satisfies $A^p = I$ and cannot be diagonalized if $\alpha \neq 0$.

Proof. □

Problem 3 (13.6.10). Let φ denote the Frobenius map $x \mapsto x^p$ on the finite field $\mathbb{F}_{p^n}$. Prove that ϕ gives an isomorphism of $\mathbb{F}_{p^n}$ to itself. Prove that φ^n is the identity map and that no lower power of φ is the identity.

Proof. □

Problem 4 (13.6.13). This exercise outlines a proof of Wedderburn's Theorem that a finite division ring D is a field.

(a) Let Z denote the center of D. Prove that Z is a field containing $\mathbb{F}_p$ for some prime p. If $Z = \mathbb{F}_q$ prove that D has order q^n for some integer n. [D is a vector space over Z].

(b) The nonzero elements $D^\times$ of D form a multiplicative group. For any $x \in D^\times$ show that the nonzero elements of D which commute with x form a division ring which contains Z. Show that this division ring is of order q^m for some integer m and that $m < n$ if x is not an element of Z.

(c) Show that the class equation for the group $D^\times$ is

$$q^n - 1 = (q-1) + \sum_{i=1}^{r} \frac{q^n - 1}{|C_{D^\times}(x_i)|}$$

where $x_1, x_2, \ldots, x_r$ are representatives of the distinct conjugacy classes in $D^\times$ not contained in the center of $D^\times$. Conclude from (b) that for each i, $|C_{D^\times}(x_i)| = q^{m_i} - 1$ for some $m_i < n$.

(d) Prove that since $\frac{q^n-1}{q^{m_i}-1}$ is an integer (namely, the index $|D^\times : C_{D^\times}(x_i)|$) then m_i divides n. Conclude that $\Phi_n(x)$ divides $(x^n - 1)/(x^{m_i} - 1)$ and hence that the integer $\Phi_n(q)$ divides $(q^n - 1)/(q^{m_i} - 1)$ for $i = 1, 2, \ldots, r$.

(e) Prove that (c) and (d)e imply that $\Phi(q) = \prod_{\zeta \text{ primitive}} (q - \zeta)$ divides $q - 1$. Prove that $|q - \zeta| > q - 1$ (complex absolute value) for any root of unity $\zeta \neq 1$ [note that 1 is the closest point on the unit circle in $\mathbb{C}$] to the point q on the real line]. Conclude that $n = 1$, i.e., that $D = Z$ is a field.

Proof. □

Problem 5 (14.1.4). Prove that $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{3}]$ are not isomorphic.

Proof. □

Problem 6 (14.2.4). Let p be a prime. Determine the elements of the Galois group of $x^p - 2$.

Proof. □

Problem 7 (14.2.5). Prove that the Galois group of $x^p - 2$ for p a prime is isomorphic to the group of matrices $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ where $a, b \in \mathbb{F}_p, a \neq 0$.

Proof. □

Problem 8 (14.2.14). Show that $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is a cyclic quartic field, i.e., is a Galois extension of degree 4 with cyclic Galois group.

Proof. □