[10.1] Prove that a *finite division* ring D (a not-necessarily commutative ring with 1 in which any non-zero element has a multiplicative inverse) is commutative. (This is due to *Wedderburn.*) (*Hint:* Check that the center k of D is a field, say of cardinality q. Let $D^\times$ act on D by conjugation, namely $\alpha \cdot \beta = \alpha\beta\alpha^{-1}$, and count orbits, to obtain an equality of the form

$$|D| = q^n = q + \sum_d \frac{q^n - 1}{q^d - 1}$$

where d is summed over some set of integers all strictly smaller than n. Let $\Phi_n(x)$ be the n^{th} cyclotomic polynomial. Show that, on one hand, $\Phi_n(q)$ divides $q^n - q$, but, on the other hand, this is impossible unless $n = 1$. Thus $D = k$.)

First, the *center* k of D is defined to be

$$k = \text{center } D = \{\alpha \in D : \alpha x = x\alpha \quad \text{for all } x \in D\}$$

We claim that k is a field. It is easy to check that k is closed under addition, multiplication, and contains 0 and 1. Since $-\alpha = (-1) \cdot \alpha$, it is closed under taking additive inverses. There is a slight amount of interest in considering closure under taking multiplicative inverses. Let $0 \neq \alpha \in k$, and $x \in D$. Then left-multiply *and* right- multiply $\alpha x = x\alpha$ by α^{-1} to obtain $x\alpha^{-1} = \alpha^{-1}x$. This much proves that k is a division ring. Since its elements commute with every $x \in D$ certainly k is commutative. This proves that k is a field.

The same argument shows that for any $x \in D$ the **centralizer**

$$D_x = \text{centralizer of } x = \{\alpha \in D : \alpha x = x\alpha\}$$

is a division ring, though possibly non-commutative. It certainly contains the center k, so is a k-vectorspace. Noting that $\alpha x = x\alpha$ is equivalent to $\alpha x \alpha^{-1} = x$ for α invertible, we see that $D_x^\times$ is the pointwise fixer of x under the conjugation action.

Thus, the orbit-counting formula gives

$$|D| = |k| + \sum_{\text{non-central orbits } O_x} [D^\times : D_x^\times]$$

where the center k is all singleton orbits and O_x is summed over orbits of non-central elements, choosing representatives x for O_x. This much did not use finiteness of D.

Let $q = |k|$, and $n = \dim_k D$. Suppose $n > 1$. Let $n_x = \dim_k D_x$. Then

$$q^n = q + \sum_{\text{non-central orbits } O_x} \frac{q^n - 1}{q^{n_x} - 1}$$

In all the non-central orbit summands, $n > n_x$. Rearranging,

$$q - 1 = -(q^n - 1) + \sum_{\text{non-central orbits } O_x} \frac{q^n - 1}{q^{n_x} - 1}$$

Let $\Phi_n(x)$ be the n^{th} cyclotomic polynomial, viewed as an element of $\mathbb{Z}[x]$. Then, from the fact that the recursive definition of $\Phi_n(x)$ really does yield a monic polynomial of positive degree with integer coefficients (and so on), and since $n_x < n$ for all non-central orbits, the integer $\Phi_n(q)$ divides the right-hand side, so divides $q - 1$.

We claim that as a complex number $|\Phi_n(q)| > q - 1$ for $n > 1$. Indeed, fix a primitive n^{th} root of unity $\zeta \in \mathbb{C}$. The set of *all* primitive n^{th} roots of unity is $\{\zeta^a\}$ where $1 \leq a \leq p$ prime to p. Then

$$|\Phi_n(q)|^2 = \prod_{a:\, \gcd(a,n)=1} |q - \zeta^a|^2 = \prod_{a:\, \gcd(a,n)=1} \left[(q - \text{Re}(\zeta^a))^2 + (\text{Im}(\zeta^a))^2\right]$$

Since $|\zeta| = 1$, the real part is certainly between -1 and $+1$, so $q - \mathrm{Re}(\zeta^a) > q - 1$ unless $\mathrm{Re}(\zeta^a) = 1$, which happens only for $\zeta^a = 1$, which can happen only for $n = 1$. That is, for $n > 1$, the integer $\Phi_n(q)$ is a product of complex numbers each larger than $q - 1$, contradicting the fact that $\Phi_n(q)|(q - 1)$. That is, $n = 1$. That is, there are no non-central orbits, and D is commutative.

[10.2] Let $q = p^n$ be a (positive integer) power of a prime p. Let $F : \mathbb{F}_q \to \mathbb{F}_q$ by $F(\alpha) = \alpha^p$ be the Frobenius map over $\mathbb{F}_p$. Let S be a set of elements of $\mathbb{F}_q$ stable under F (that is, F maps S to itself). Show that the polynomial

$$\prod_{\alpha \in S} (x - \alpha)$$

has coefficients in the smaller field $\mathbb{F}_p$.

Since the set S is Frobenius-stable, application of the Frobenius to the polynomial merely permutes the linear factors, thus leaving the polynomial unchanged (since the multiplication of the linear factors is insensitive to ordering.) Thus, the coefficients of the (multiplied-out) polynomial are fixed by the Frobenius. That is, the coefficients are roots of the equation $x^p - x = 0$. On one hand, this polynomial equation has at most p roots in a given field (from unique factorization), and, on the other hand, Fermat's Little Theorem assures that the elements of the field $\mathbb{F}_p$ are roots of that equation. Thus, any element fixed under the Frobenius lies in the field $\mathbb{F}_p$, as asserted.

[10.3] Let $q = p^n$ be a power of a prime p. Let $F : \mathbb{F}_q \to \mathbb{F}_q$ by $F(\alpha) = \alpha^p$ be the Frobenius map over $\mathbb{F}_p$. Show that for every divisor d of n that the fixed points of F^d form the unique subfield $\mathbb{F}_{p^d}$ of $\mathbb{F}_q$ of degree d over the prime field $\mathbb{F}_p$.

This is similar to the previous example, but emphasizing a different part. Fixed points of the d^{th} power F^d of the Frobenius F are exactly the roots of the equation $x^{p^d} - x = 0$ of $x(x^{p^d - 1} - 1) = 0$. On one hand, a polynomial has at most as many roots (in a field) as its degree. On the other hand, $\mathbb{F}_{p^d}^\times$ is of order $p^d - 1$, so every element of $\mathbb{F}_{p^d}$ is a root of our equation. There can be no more, so $\mathbb{F}_{p^d}$ is exactly the set of roots.

[10.4] Let $f(x)$ be a monic polynomial with integer coefficients. Show that f is irreducible in $\mathbb{Q}[x]$ if it is irreducible in $(\mathbb{Z}/p)[x]$ for some p.

First, claim that if $f(x)$ is irreducible in some $(\mathbb{Z}/p)[x]$, then it is irreducible in $\mathbb{Z}[x]$. A factorization $f(x) = g(x) \cdot h(x)$ in $\mathbb{Z}[x]$ maps, under the natural $\mathbb{Z}$-algebra homomorphism to $(\mathbb{Z}/p)[x]$, to the corresponding factorization $f(x) = g(x) \cdot h(x)$ in $(\mathbb{Z}/p)[x]$. (There's little reason to invent a notation for the reduction modulo p of polynomials as long as we are clear what we're doing.) A critical point is that since f is monic both g and h can be taken to be monic also (multiplying by -1 if necessary), since the highest-degree coefficient of a product is simply the product of the highest-degree coefficients of the factors. The irreducibility over $\mathbb{Z}/p$ implies that the degree of one of g and h modulo p is 0. Since they are monic, reduction modulo p does not alter their degrees. Since f is monic, its content is 1, so, by Gauss' lemma, the factorization in $\mathbb{Z}[x]$ is not proper, in the sense that either g or h is just ± 1.

That is, f is irreducible in the ring $\mathbb{Z}[x]$. Again by Gauss' lemma, this implies that f is irreducible in $\mathbb{Q}[x]$.

[10.5] Let n be a positive integer such that $(\mathbb{Z}/n)^\times$ is *not* cyclic. Show that the n^{th} cyclotomic polynomial $\Phi_n(x)$ factors properly in $\mathbb{F}_p[x]$ for any prime p not dividing n.

(See subsequent text for systematic treatment of the case that p divides n.) Let d be a positive integer such that $p^d - 1 = 0 \bmod n$. Since we know that $\mathbb{F}_{p^d}^\times$ is cyclic, $\Phi_n(x) = 0$ has a root in $\mathbb{F}_{p^d}$ when $p^d - 1 = 0 \bmod n$. For $\Phi_n(x)$ to be irreducible in $\mathbb{F}_p[x]$, it must be that $d = \varphi(n)$ (Euler's totient function φ) is the smallest exponent which achieves this. That is, $\Phi_n(x)$ will be irreducible in $\mathbb{F}_p[x]$ only if $p^{\varphi(n)} = 1 \bmod n$ but no smaller positive exponent achieves this effect. That is, $\Phi_n(x)$ is irreducible in $\mathbb{F}_p[x]$ only if p is of order $\varphi(n)$ in the group $(\mathbb{Z}/n)^\times$. We know that the order of this group is $\varphi(n)$, so any such p would be a generator for the group $(\mathbb{Z}/n)^\times$. That is, the group would be cyclic.

[10.6] Show that the 15^{th} cyclotomic polynomial $\Phi_{15}(x)$ is irreducible in $\mathbb{Q}[x]$, despite being reducible in $\mathbb{F}_p[x]$ for every prime p.

First, by Sun-Ze

$$(\mathbb{Z}/15)^\times \approx (\mathbb{Z}/3)^\times \times (\mathbb{Z}/5)^\times \approx \mathbb{Z}/2 \oplus \mathbb{Z}/4$$

This is not cyclic (there is no element of order 8, as the maximal order is 4). Thus, by the previous problem, there is no prime p such that $\Phi_{15}(x)$ is irreducible in $\mathbb{F}_p[x]$.

To prove that Φ_{15} is irreducible in $\mathbb{Q}[x]$, it suffices to show that the field extension $\mathbb{Q}(\zeta)$ of $\mathbb{Q}$ generated by any root ζ of $\Phi_{15}(x) = 0$ (in some algebraic closure of $\mathbb{Q}$, if one likes) is of degree equal to the degree of the polynomial Φ_{15}, namely $\varphi(15) = \varphi(3)\varphi(5) = (3-1)(5-1) = 8$. We already know that Φ_3 and Φ_5 are irreducible. And one notes that, given a primitive 15^{th} root of unity ζ, $\eta = \zeta^3$ is a primitive 5^{th} root of unity and $\omega = \zeta^5$ is a primitive third root of unity. And, given a primitive cube root of unity ω and a primitive 5^{th} root of unity η, $\zeta = \omega^2 \cdot \eta^{-3}$ is a primitive 15^{th} root of unity: in fact, if ω and η are produced from ζ, then this formula recovers ζ, since

$$2 \cdot 5 - 3 \cdot 3 = 1$$

Thus,

$$\mathbb{Q}(\zeta) = \mathbb{Q}(\omega)(\eta)$$

By the multiplicativity of degrees in towers of fields

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}(\omega)] \cdot [\mathbb{Q}(\omega) : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}(\omega)] \cdot 2 = [\mathbb{Q}(\omega, \eta) : \mathbb{Q}(\omega)] \cdot 2$$

Thus, it would suffice to show that $[\mathbb{Q}(\omega, \eta) : \mathbb{Q}(\omega)] = 4$.

We should not forget that we have shown that $\mathbb{Z}[\omega]$ is Euclidean, hence a PID, hence a UFD. Thus, we are entitled to use Eisenstein's criterion and Gauss' lemma. Thus, it would suffice to prove irreducibility of $\Phi_5(x)$ in $\mathbb{Z}[\omega][x]$. As in the discussion of $\Phi_p(x)$ over $\mathbb{Z}$ with p prime, consider $f(x) = \Phi_5(x+1)$. All its coefficients are divisible by 5, and the constant coefficient is exactly 5 (in particular, not divisible by 5^2). We can apply Eisenstein's criterion and Gauss' lemma if we know, for example, that 5 is a prime in $\mathbb{Z}[\omega]$. (There are other ways to succeed, but this would be simplest.)

To prove that 5 is prime in $\mathbb{Z}[\omega]$, recall the *norm*

$$N(a + b\omega) = (a + b\omega)(a + b\overline{\omega}) = (a + b\omega)(a + b\omega^2) = a^2 - ab + b^2$$

already used in discussing the Euclidean-ness of $\mathbb{Z}[\omega]$. One proves that the norm takes non-negative integer values, is 0 only when evaluated at 0, is *multiplicative* in the sense that $N(\alpha\beta) = N(\alpha)N(\beta)$, and $N(\alpha) = 1$ if and only if α is a unit in $\mathbb{Z}[\omega]$. Thus, if 5 were to factor $5 = \alpha\beta$ in $\mathbb{Z}[\omega]$, then

$$25 = N(5) = N(\alpha) \cdot N(\beta)$$

For a proper factorization, meaning that neither α nor β is a unit, neither $N(\alpha)$ nor $N(\beta)$ can be 1. Thus, both must be 5. However, the equation

$$5 = N(a + b\omega) = a^2 - ab + b^2 = (a - \frac{b}{2})^2 + \frac{3}{4}b^2 = \frac{1}{4}\left((2a-b)^2 + 3b^2\right)$$

has no solution in integers a, b. Indeed, looking at this equation mod 5, since 3 is not a square mod 5 it must be that $b = 0$ mod 5. Then, further, $4a^2 = 0$ mod 5, so $a = 0$ mod 5. That is, 5 divides both a and b. But then 25 divides the norm $N(a + b\omega) = a^2 - ab + b^2$, so it cannot be 5.

Thus, in summary, 5 is prime in $\mathbb{Z}[\omega]$, so we can apply Eisenstein's criterion to $\Phi_5(x+1)$ to see that it is irreducible in $\mathbb{Z}[\omega][x]$. By Gauss' lemma, it is irreducible in $\mathbb{Q}(\omega)[x]$, so $[\mathbb{Q}(\omega, \eta) : \mathbb{Q}(\omega)] = \varphi(5) = 4$. And this proves that $[\mathbb{Q}(\zeta) : \mathbb{Q})] = 8$, so $\Phi_{15}(x)$ is irreducible over $\mathbb{Q}$.

[10.7] Let p be a prime. Show that every degree d irreducible in $\mathbb{F}_p[x]$ is a factor of $x^{p^d-1}-1$. Show that that the $(p^d-1)^{th}$ cyclotomic polynomial's irreducible factors in $\mathbb{F}_p[x]$ are all of degree d.

Let $f(x)$ be a degree d irreducible in $\mathbb{F}_p[x]$. For a linear factor $x-\alpha$ with α in some field extension of $\mathbb{F}_p$, we know that

$$[\mathbb{F}_p(\alpha):\mathbb{F}_p] = \text{ degree of minimal poly of } \alpha = \deg f = d$$

Since there is a unique (up to isomorphism) field extension of degree d of $\mathbb{F}_p$, *all* roots of $f(x)=0$ lie in that field extension $\mathbb{F}_{p^d}$. Since the order of the multiplicative group $\mathbb{F}_{p^d}^\times$ is p^d-1, by Lagrange the order of any non-zero element α of $\mathbb{F}_{p^d}$ is a divisor of p^d-1. That is, α is a root of $x^{p^d-1}-1=0$, so $x-\alpha$ divides $x^{p^d-1}-1=0$. Since f is irreducible, f has no repeated factors, so $f(x)=0$ has no repeated roots. By unique factorization (these linear factors are mutually distinct irreducibles whose least common multiple is their product), the product of all the $x-\alpha$ divides $x^{p^d-1}-1$.

For the second part, similarly, look at the linear factors $x-\alpha$ of $\Phi_{p^d-1}(x)$ in a sufficiently large field extension of $\mathbb{F}_p$. Since p does not divide $n=p^d-1$ there are no repeated factors. The multiplicative group of the field $\mathbb{F}_{p^d}$ is *cyclic*, so contains exactly $\varphi(p^d-1)$ elements of (maximal possible) order p^d-1, which are roots of $\Phi_{p^d-1}(x)=0$. The degree of Φ_{p^d-1} is $\varphi(p^d-1)$, so there are no *other* roots. No proper subfield $\mathbb{F}_{p^e}$ of $\mathbb{F}_{p^d}$ contains *any* elements of order p^d-1, since we know that $e|d$ and the multiplicative group $\mathbb{F}_{p^e}^\times$ is of order $p^e-1<p^d-1$. Thus, any linear factor $x-\alpha$ of $\Phi_{p^d-1}(x)$ has $[\mathbb{F}_p(\alpha):\mathbb{F}_p]=d$, so the minimal polynomial $f(x)$ of α over $\mathbb{F}_p$ is necessarily of degree d. We claim that f divides Φ_{p^d-1}. Write

$$\Phi_{p^d-1} = q\cdot f + r$$

where q,r are in $\mathbb{F}_p[x]$ and $\deg r<\deg f$. Evaluate both sides to find $r(\alpha)=0$. Since f was minimal over $\mathbb{F}_p$ for α, necessarily $r=0$ and f divides the cyclotomic polynomial.

That is, any linear factor of Φ_{p^d-1} (over a field extension) is a factor of a degree d irreducible polynomial in $\mathbb{F}_p[x]$. That is, that cyclotomic polynomial factors into degree d irreducibles in $\mathbb{F}_p[x]$.

[10.8] Fix a prime p, and let ζ be a primitive p^{th} root of 1 (that is, $\zeta^p=1$ and no smaller exponent will do). Let

$$V = \det\begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & \zeta & \zeta^2 & \zeta^3 & \dots & \zeta^{p-1} \\ 1 & \zeta^2 & (\zeta^2)^2 & (\zeta^2)^3 & \dots & (\zeta^2)^{p-1} \\ 1 & \zeta^3 & (\zeta^3)^2 & (\zeta^3)^3 & \dots & (\zeta^3)^{p-1} \\ 1 & \zeta^4 & (\zeta^4)^2 & (\zeta^4)^3 & \dots & (\zeta^4)^{p-1} \\ \vdots & & & & & \vdots \\ 1 & \zeta^{p-1} & (\zeta^{p-1})^2 & (\zeta^{p-1})^3 & \dots & (\zeta^{p-1})^{p-1} \end{pmatrix}$$

Compute the rational number V^2.

There are other possibly more natural approaches as well, but the following trick is worth noting. The ij^{th} entry of V is $\zeta^{(i-1)(j-1)}$. Thus, the ij^{th} entry of the square V^2 is

$$\sum_\ell \zeta^{(i-1)(\ell-1)}\cdot\zeta^{(\ell-1)(j-1)} = \sum_\ell \zeta^{(i-1+j-1)(\ell-1)} = \begin{cases} 0 & \text{if } (i-1)+(j-1)\neq 0 \bmod p \\ p & \text{if } (i-1)+(j-1)=0 \bmod p \end{cases}$$

since

$$\sum_{0\le\ell<p} \omega^\ell = 0$$

for any p^{th} root of unity ω other than 1. Thus,

$$V^2 = \begin{pmatrix} p & 0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 0 & \ldots & 0 & p \\ 0 & 0 & 0 & \ldots & p & 0 \\ & & & \iddots & & \\ 0 & 0 & p & \ldots & 0 & 0 \\ 0 & p & 0 & \ldots & 0 & 0 \end{pmatrix}$$

That is, there is a p in the upper left corner, and p's along the anti-diagonal in the lower right $(n-1)$-by-$(n-1)$ block. Thus, granting that the determinant squared is the square of the determinant,

$$(\det V)^2 = \det(V^2) = p^p \cdot (-1)^{(p-1)(p-2)/2}$$

Note that this did not, in fact, depend upon p being prime.

[10.9] Let $K = \mathbb{Q}(\zeta)$ where ζ is a primitive 15^{th} root of unity. Find 4 fields k strictly between $\mathbb{Q}$ and K.

Let ζ be a primitive 15^{th} root of unity. Then $\omega = \zeta^5$ is a primitive cube root of unity, and $\eta = \zeta^3$ is a primitive fifth root of unity. And $\mathbb{Q}(\zeta) = \mathbb{Q}(\omega)(\eta)$.

Thus, $\mathbb{Q}(\omega)$ is one intermediate field, of degree 2 over $\mathbb{Q}$. And $\mathbb{Q}(\eta)$ is an intermediate field, of degree 4 over $\mathbb{Q}$ (so certainly distinct from $\mathbb{Q}(\omega)$.)

By now we know that $\sqrt{5} \in \mathbb{Q}(\eta)$, so $\mathbb{Q}(\sqrt{5})$ suggests itself as a third intermediate field. But one must be sure that $\mathbb{Q}(\omega) \neq \mathbb{Q}(\sqrt{5})$. We can try a direct computational approach in this simple case: suppose $(a + b\omega)^2 = 5$ with rational a, b. Then

$$5 = a^2 + 2ab\omega + b^2\omega^2 = a^2 + 2ab\omega - b^2 - b^2\omega = (a^2 - b^2) + \omega(2ab - b^2)$$

Thus, $2ab - b^2 = 0$. This requires either $b = 0$ or $2a - b = 0$. Certainly b cannot be 0, or 5 would be the square of a rational number (which we have long ago seen impossible). Try $2a = b$. Then, supposedly,

$$5 = a^2 - 2(2a)^2 = -3a^2$$

which is impossible. Thus, $\mathbb{Q}(\sqrt{5})$ is distinct from $\mathbb{Q}(\omega)$.

We know that $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$. This might suggest

$$\mathbb{Q}(\sqrt{-3} \cdot \sqrt{5}) = \mathbb{Q}(\sqrt{-15})$$

as the fourth intermediate field. We must show that it is distinct from $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{5})$. If it were equal to either of these, then that field would also contain $\sqrt{5}$ and $\sqrt{-3}$, but we have already checked that (in effect) there is no quadratic field extension of $\mathbb{Q}$ containing both these.

Thus, there are (at least) intermediate fields $\mathbb{Q}(\eta)$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{5}$, and $\mathbb{Q}(\sqrt{-15})$.