Kenneth Ireland & Michael Rosen A Classical Introduction to Modern Number Theory (Chapter 7 Solutions)

Khang Vinh Nguyen

March 23, 2022

Exercise 1. Use the method of Theorem 1 to show that a finite subgroup of the multiplicative group of a field is cyclic.

Proof. Let G be a finite subgroup of $F^\times$ of order n. Then for any d divides n, since $x^d = 1$ only has at most d roots in a field, we know that $|\{x \in G : x^d = 1\}| \leq d$. If there exists an element α of order d, then it generates a subset of $\{x \in G : x^d = 1\}$ of cardinality d. From the previous inequality, we conclude that α generates the group $\{x \in G : x^d = 1\}$. This group is obviously cyclic of order d so there are exactly $\varphi(d)$ generators.

So either there are none, or there are $\varphi(d)$ elements in G of order d. However, the order of G is n, and each element has an order divide n, so

$$n \leq \sum_{d|n} \varphi(d) = n$$

In other words, the equality holds, so in particular, there are $\varphi(n)$ elements of order n. We conlcude that G is cyclic. □

Exercise 2. Let $\mathbb{R}$ and $\mathbb{C}$ be the real and complex numbers, respectively. Find the finite subgroups of $\mathbb{R}^*$ and $\mathbb{C}^*$ and show directiy that they are cyclic.

Proof. For $\mathbb{R}$, suppose G is a finite subgroup of $\mathbb{R}^*$. Then every element of G has finite order. However, the only non-zero real numbers of finite order are $\{\pm 1\}$, so either $G = \{1\}$ (trivially cyclic) or $G = \{\pm 1\}$ (generates by -1).

*For $\mathbb{C}$, suppose G is a finite subgroup of $\mathbb{C}^*$. Then again, every element of G has finite order. Consider $z^n = 1$, then we know that $e^{\frac{2\pi ik}{n}}$ for integers $0 \leq k < n$ are all non-zero complex numbers of finite order. Pick $e^{\frac{2\pi ik}{n}} \in G$ so that $\gcd(k, n) = 1$ and n is largest (as G only has finitely many elements). Then evert n-th root of unity must be in G, and we will show those are all element in G.

Let $e^{\frac{2\pi il}{d}}$ with $\gcd(l, d) = 1$ be a number in G, then $d \leq n$ by maximality. If $d \nmid n$, then there exists some prime divisor p of d that does not divide n. Multiplying if necessary, we should get $e^{\frac{2\pi i}{p}} \in G$ and similarly, $e^{\frac{2\pi i}{n}} \in G$. But since

$$\frac{1}{p} + \frac{1}{n} = \frac{p+n}{pn}$$

is at reduced form (indeed, if $d \mid p+n, pn$, then $d \mid p^2$, and so $d = 1$ since $p \nmid n$), we have a contradiction to maximality of n.

In other words, if $e^{\frac{2\pi il}{d}} \in G$ (with $\gcd(l, d) = 1$), then $d \mid n$. We conclude that G is cyclic of order n. □

Exercise 3. Let F be a field with q elements and suppose that $q \equiv 1 \pmod{n}$. Show that for $\alpha \in F^*$, the equation $x^n = \alpha$ has either no solutions or n solutions.

Proof. We show that if it has solution, then it has n solution. Note that the equation $x^n = 1$ has exactly n solution in F^* since n divides the order of F^*, which is $q-1$ (also because F^* is cyclic). Thus given some $t^n = \alpha$, we have $(tz)^n = \alpha$ for each $z^n = 1$. Since neither t nor z is zero, we get n distinct solutions. However the polynomial $x^n - \alpha$ has at most n solution, as F is an integral domain, so we conclude that $x^n = \alpha$ has n solutions. □

Exercise 4 (continuation)**.** Show that the set of $\alpha \in F^*$ such that $x^n = \alpha$ is solvable is a subgroup with $(q-1)/n$ elements.

Proof. Given $\alpha = t^n$ and $\beta = s^n$ for some $t, s \in F^*$, then we have $\alpha\beta^{-1} = (ts^{-1})^n$, so such set S is a subgroup of F^*. Define the following map

$$F^* \to F^*$$

$$x \mapsto x^n$$

We know that the image of the map is S, while each non-empty fiber (where $x^n = \alpha$ is solvable) has exactly n elements (Exercise 3). Thus, $|F^*| = n|S|$, or equivalently, $|S| = \frac{q-1}{n}$. □

Exercise 5 (continuation)**.** Let K be a field containing F such that $[K : F] = n$. For all $\alpha \in F^*$, show that the equation $x^n = \alpha$ has n solutions in K. [Hint: Show that $q^n - 1$ is divisible by $n(q-1)$ and use the fact that $\alpha^{q-1} = 1$.]

Proof. If $x^n = \alpha$ has n solutions in K for each $\alpha \in F^*$, each such satisfies $x^{n(q-1)} = \alpha^{q-1} = 1$, so $\{x \in K^* : x^{n(q-1)} = 1\}$ has exactly $n(q-1)$ elements. This should tell us to show that $q^n - 1$ (the order of K^*) is divisible by $n(q-1)$.

Indeed, still assume $q \equiv 1 \pmod{n}$, we then get $q^{n-1} + q^{n-2} + \cdots + 1 \equiv n \equiv 0 \pmod{n}$, so $(q-1)n \mid (q-1)(q^{n-1} + q^{n-2} + \cdots + 1) = q^n - 1$. But K^* is cylic, so there is a subgroup of order $n(q-1)$. In other words, $x^{n(q-1)} = 1$ has exactly $n(q-1)$ solutions in K.

*Since $F^* \subseteq K^*$, every equation $x^n = \alpha$ either has no solution or n solutions in K (Exercise 3), together with the fact that $n \mid n(q-1) \mid q^n - 1$). Each such solution for some $\alpha \in F^*$, will lead to a solution of $x^{n(q-1)} = 1$, since $x^{n(q-1)} = \alpha^{q-1} = 1$ (where $|F^*| = q-1$). Vice versa, if $x^{n(q-1)} = 1$, then $(x^n)^{q-1} = 1$, so $x^n \in F^*$.

Now let $C_\alpha \in \{0, n\}$ be the number of solutions of $x^n = \alpha$ in K, we get

$$n(q-1) \leq \sum_{\alpha \in F^*} C_\alpha \leq n|F^*| = n(q-1)$$

Equality happens, and so $C_\alpha = n$. □

Exercise 6. Let $K \supseteq F$ be finite fields with $[K : F] = 3$. Show that if $\alpha \in F$ is not a square in F, it is not a square in K.

Proof. Note that $x^2 - \alpha$ is irreducible over F since it is quadratic, and there is no root of it in F. Thus, the splitting field H is a degree 2 extension of F. If K contains a square root of α, then $x^2 - \alpha$ splits in K, so H must be a subfield of K. Yet

$$3 = [K : F] = [K : H][H : F] = 2[K : H]$$

which is impossible □

Exercise 7. Generalize Exericse 6 by showing that if α is not a square in F, it is not a square in any extension of odd degree and is a square in every extension of even degree.

Proof. The odd degree is clear since it cannot equal to any even number. As for even degree, suppose $[K : F] = 2n$. Then if $|F| = q$, we get $|K| = q^{2n}$. Note that $x^2 - \alpha$ is monic and irreducible over F, and $2 \mid 2n$, so $x^2 - \alpha \mid x^{q^{2n}} - x$. But $x^{q^{2n}} - x$ splits in K, so $x^2 - \alpha$ also splits completely in K, and so α is a square in K. □

Exercise 8. In a field with 2^n elements what is the subgroup of squares?

Proof. Consider the Frobenius map on F

$$x \mapsto x^2$$

It is field homomorphism since $(x+y)^2 = x^2 + 2xy + y^2 = x^2 + y^2$, and $(xy)^2 = x^2y^2$. It is also injective since $x^2 = y^2$ iff $x^2 - y^2 = (x-y)^2 = 0$ iff $x = y$, so since F is finite, the map is a also surjective. Since 0 maps to 0, the rest maps to themselves. In other word, the subgroup of squares is exactly the multiplicative group F^*. □

Exercise 9. If $K \supseteq F$ are finite fields, $|F| = q, \alpha \in F, q \equiv 1 \pmod{n}$, and $x^n = \alpha$ is not solvable in F, show that $x^n = \alpha$ is not solvable in K if $\gcd(n, [K : F]) = 1$.

Proof. We show that $x^n = \alpha$ has a solution in a field F of q elements iff $\alpha^{\frac{q-1}{n}} = 1$ (assuming $\alpha \neq 0$, and $n \mid q-1$). Suppose $x_0^n = \alpha$ for some $x_0 \in F$, then $\alpha^{\frac{q-1}{n}} = x_0^{q-1} = 1$. Vice versa, suppose $\alpha^{\frac{q-1}{n}} = 1$, then α is an element of the subgroup of order $\frac{q-1}{n}$ in K^*. But if g generates K^*, then g^n generates the subgroup of order $\frac{q-1}{n}$, so $g^{nk} = \alpha$ for some $k \leq \frac{q-1}{n}$. Letting $x = g^k$, then we get a solution to $x^n = \alpha$.

Thus, suppose $x^n = \alpha$ is solvable in K. Then $\alpha^{\frac{q^m-1}{n}} = 1$, where $|K| = q^m$ (and so $[K : F] = m$). However, $x^n = \alpha$ is not solvable in F, so $\beta = \alpha^{\frac{q-1}{n}} \neq 1$. Now note that $\beta^{q^{m-1}+\cdots+q+1} = \alpha^{\frac{q^m-1}{n}} = 1$. On the other hand, $\beta^n = \alpha^{q-1} = 1$ (since $\alpha \in F$, and $\alpha \neq 0$ due to $x^n = \alpha$ is not solvable in F).

We then must have $\gcd(q^{m-1}+\cdots+q+1, n) > 1$, as $\beta \neq 1$. But $q \equiv 1 \pmod{n}$, so $q^{m-1} + \cdots + q + 1 \equiv m \pmod{n}$. From there, $\gcd(q^{m-1} + \cdots + q + 1, n) = \gcd(m, n) > 1$. By contraposition, we have Q.E.D. □

Exercise 10. Let $K \supseteq F$ be finite fields and $[K : F] = 2$ (with $|F| = q$). For $\beta \in K$ show that $\beta^{1+q} \in F$ and moreover that every element in F is of the form β^{1+q} for some $\beta \in K$.

Proof. If $\beta = 0$, then $\beta^{1+q} = 0 \in F$. Otherwise, $\beta^{q^2-1} = 1$ (since $|K| = q^2$), so $(\beta^{q+1})^{q-1} = 1$. But any $\alpha^{q-1} = 1$ must imply that $\alpha \in F$, so we have $\beta^{q+1} \in F$. On the other hand, by Exercise 3, the equation $x^{q+1} = \alpha \in F^*$ has either no solution or $q+1$ solutions in K (as $q+1 \mid q^2-1$).

Denoting $C_\alpha \in \{0, q+1\}$ to be the solutions of $x^{q+1} = \alpha$, we get

$$q^2 - 1 = \sum_{\alpha \in F^*} C_\alpha \leq (q+1)|F^*| = q^2 - 1$$

Thus, $C_\alpha = q + 1$ for all $\alpha \in F^*$. □

Exercise 11. With the situation being that of Exercise 10 suppose that $\alpha \in F$ has order $q-1$. Show that there is a $\beta \in K$ with order q^2-1 such that $\beta^{1+q} = \alpha$.

This is just purely group theory, so we prove the following lemmas

Lemma 11.1. Given $\gcd(k, d) = 1$ and $d \mid n$ (with $d \neq 0$), there exists some integer l such that $k \equiv l \pmod{d}$ and $\gcd(l, n) = 1$

Proof. Let $p_1, p_2, \ldots, p_r$ be all prime factors of n that is not a factor of d. By Chinese remainder theorem, there exists some l satisfying following congruences

$$l \equiv k \pmod{d} \text{ and } l \equiv 1 \pmod{p_i}, 1 \leq i \leq r$$

For each prime divisor q of n, if $q \mid d$, then $\gcd(l, q) = \gcd(k, q) = 1$ since $\gcd(k, d) = 1$. Otherwise, $q \nmid d$, so it must be some p_i above. But since $l \equiv 1 \pmod{p_i}$, we have $\gcd(l, q) = \gcd(1, p_i) = 1$. Therefore, l is not divisible by any prime factor of n, so $\gcd(l, n) = 1$. □

Lemma 11.2. Given G is cylic group of order n, and α generates a subgroup of order d, then there exists a generator β of G such that $\alpha = \beta^{n/d}$.

Proof. Let g be a generator of G. Since there is only one subgroup of order d in G, we know that $g^{(n/d)k} = \alpha$ for some $0 \leq k \leq d-1$. Note that $\alpha = g^{(n/d)k}$ has order d, k must be relatively prime to d. By the previous lemma, there must be some $l \equiv k \pmod{d}$ such that $\gcd(l, n) = 1$. We then denote $\beta = g^l$, which is of order n. On the other hand, $k \equiv l \pmod{d}$, so $(n/d)k \equiv (n/d)l \pmod{n}$, so we have $\beta^{n/d} = g^{(n/d)l} = g^{(n/d)k} = \alpha$. □

Solution to the original. By the hypothesis, α still has order $q-1$ in K^*. Since K^* is cyclic of order $q^2 - 1$, the previous lemma should give us some β of order $q^2 - 1$ such that

$$\beta^{q+1} = \beta^{\frac{q^2-1}{q-1}} = \alpha$$

□

Exercise 12. Use Proposition 7.2.1 to show that given a field k and a polynomial $f(x) \in k[x]$ there is a field $K \supseteq k$ such that $[K : k]$ is finite and $f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ in $K[x]$.

Proof. We use induction on the degree of $f(x)$. If $\deg f(x) = 1$, then $K = k$ should be suffice. Assuming, $\deg f(x) = k + 1$, then there exists a field K containing k such that $f(\alpha) = 0$ for some $\alpha \in K$. Since $f(x)$ can be lift to a polynomial over K, we can factor $(x - \alpha)$ out, so that there exists some $g(x) \in K[x]$ such that $f(x) = (x - \alpha)g(x)$. Since $\deg g(x) = k$, we can find another field L containing K such that $g(x) = (x - \beta_1)(x - \beta_2) \cdots (x - \beta_k)$ in K by induction. $\square$

Exercise 14. Let F be a field with q elements and n a positive integer. Show that there exist irreducible polynomials in $F[x]$ of degree n.

Proof. We know that there is a field K containing F such that K has q^n elements. Let α be a generator of K^*, then $K = F(\alpha)$. If $f(x)$ is the minimal polynomial of α over F, then $n = [K : F] = [F(\alpha) : F] = \deg f(x)$. In other words, $f(x)$ is an irreducible polynomial of degree n. □

Exercise 15. Let $x^n - 1 \in F[x]$, where F is a finite field with q elements. Suppose that $\gcd(q, n) = 1$. Show that $x^n - 1$ splits into linear factors in some extension field and that the least degree of such a field is the smallest integer f such that $q^f \equiv 1 \pmod{n}$.

Proof. Let K be the splitting field of $x^n - 1$ over F. Suppose $|K| = q^f$, then $x^n - 1 \mid x^{q^f} - x = (x^{q^f-1} - 1)x$. Since $\gcd(x^n - 1, x) = 1$, we know that $x^n - 1 \mid x^{q^f-1} - 1$. Now consider the subset $G = \{x \in K : x^n = 1\}$ of K^*, which has n elements: one can very that G is a group, so the order of G divides K^*. In other words, $n \mid q^f - 1$.

We now show that f is the least such positive integer. Indeed, since $\gcd(q, n) = 1$, let e be the order of q modulo n. Then $n \mid q^e - 1$, so consider the finite field L of q^e elements: it is an extension of F (since F has q elements), and there is a subgroup of L of order n (note L^* is cyclic). Thus, $x^n - 1$ splits in L. By minimality, K must be a subfield of L, which shows that $f \leq e$. Since $q^f \equiv 1 \pmod{n}$, we have $e = f$ (by definition of multiplicative order modulo n). $\square$

Exercise 16. Calculate the monic irreducible polynomials of degree 4 in $\mathbb{Z}/2\mathbb{Z}[x]$.

Proof. Such polynomial cannot have 0 as root, so the constant coefficient must be 1. Also, such polynomial cannot have 1 as root, so the sum of coefficients (which are either 0 or 1) must be odd. In other words, there are odd number of terms in the polynomial, which left us with 4 possibilities

$$x^4 + x^3 + 1, x^4 + x^2 + 1, x^4 + x + 1, x^4 + x^3 + x^2 + x + 1$$

Now some of them may factor into 2 quadratics, neither of which has roots. But the only quadratic polynomial over $\mathbb{Z}/2\mathbb{Z}$ that has no root is $x^2 + x + 1$, so such polynomial must be $(x^2 + x + 1)^2 = x^4 + x^2 + 1$. Thus, this eliminates one polynomial among the previous 4, and we get 3 irreducible polynomials

$$x^4 + x^3 + 1, x^4 + x + 1, x^4 + x^3 + x^2 + x + 1$$

□

Exercise 17. Let q and p be distinct odd primes. Show that the number of monic irreducibles of degree q in $\mathbb{Z}/p\mathbb{Z}[x]$ is $q^{-1}(p^q - p)$.

Proof. Since the number of monic irreducible polynomails of degree n is

$$N_n = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d$$

Substitute $n = q$, and we get $N_q = \frac{1}{q}(\mu(q)p + \mu(1)p^q) = \frac{1}{q}(p^q - p)$. □

Exercise 18. Let p be a prime with $p \equiv 3 \pmod 4$. Show that the residue classes modulo p in $\mathbb{Z}[i]$ form a field with p^2 elements.

Proof. By assumption, p is a prime in $\mathbb{Z}[i]$, and since $\mathbb{Z}[i]$ is Euclidean, it implies that (p) is maximal, thus $\mathbb{Z}[i]/(p)$ is a finite field.

Now note that for a given integer n, $a + bi \equiv c + di \pmod n$ if there is some $r + si \in \mathbb{Z}[i]$ such that $n(r + si) = (a + bi) - (c + di)$. Equivalently, $a - c = nr$ and $b - d = ns$, so a must be congruent to c and b must be congruent to d modulo n. Thus, $\mathbb{Z}[i]/(n) = \{a + bi + (n) : 0 \leq a < n, 0 \leq b < n\}$, of which there are exactly n^2 distinct elements. Substituting $n = p$ should get us a finite field $\mathbb{Z}[i]/(p)$ of p^2 elements. □

Exercise 19. Let F be a finite field with q elements. If $f(x) \in F[x]$ has degree t, put $|f| = q^t$. Verify the formal identity $\sum_f |f|^{-s} = (1 - q^{1-s})^{-1}$. The sum is over all monic polynomials.

Proof. By counting the number of ways each coefficient (except leading coefficient, since we require a polynomial to be monic) can take in F, we have q^t monic polynomials of degree t over F. Hence

$$\sum_f |f|^{-s} = \sum_{t=0}^{\infty} q^t \cdot (q^t)^{-s} = \sum_{t=0}^{\infty} (q^{1-s})^t = \frac{1}{1 - q^{1-s}}$$

□

Exercise 20. With the notation of Exereise 19, let $d(f)$ be the number of monic divisors of f and $\sigma(f) = \sum_{g|f} |g|$ where the sum is over the monic divisors of f. Verify the following identities:

1. $\sum_f d(f)|f|^{-s} = (1-q^{1-s})^{-2}$.
2. $\sum_f \sigma(f)|f|^{-s} = (1-q^{1-s})^{-1}(1-q^{2-s})^{-1}$.

Proof. We use the idea from Dirichlet series as follows: if $\alpha, \beta : \mathcal{M} \to \mathbb{C}$ are maps from the set of monic polynomials $\mathcal{M}$ over (a finite field) F to $\mathbb{C}$, then

$$\begin{aligned}\left(\sum_f \frac{\alpha(f)}{|f|^s}\right)\left(\sum_g \frac{\beta(g)}{|g|^s}\right) &= \sum_{f,g} \frac{\alpha(f)\beta(g)}{|f|^s|g|^s} = \sum_{f,g} \frac{\alpha(f)\beta(g)}{q^{s(\deg f + \deg g)}} \\ &= \sum_{f,g} \frac{\alpha(f)\beta(g)}{q^{s\deg(fg)}} = \sum_{f,g} \frac{\alpha(f)\beta(g)}{|fg|^s} \\ &= \sum_h \frac{1}{|h|^s} \sum_{fg=h} \alpha(f)\beta(g) \\ &= \sum_h \frac{(\alpha * \beta)(h)}{|h|^s}\end{aligned}$$

where $(\alpha*\beta)(h) = \sum_{fg=h} \alpha(f)\beta(g) = \sum_{f|h} \alpha(f)\beta\left(\frac{h}{f}\right)$ is the Dirichlet convolution of α and β.

Part 1: since $d(f) = \sum_{g|f} 1 = (1*1)(f)$ (where $1(f) = 1$ for all f monic), so

$$\sum_f d(f)|f|^{-s} = \left(\sum_f |f|^{-s}\right)^2 = \frac{1}{(1-q^{1-s})^2}$$

Part 2: since $\sigma(f) = \sum_{g|f} |g|$ is the convolution of the maps $1(g)$ and $|g|$, we get

$$\begin{aligned}\sum_f \sigma(f)|f|^{-s} &= \left(\sum_f |f|^{-s}\right)\left(\sum_f |f| \cdot |f|^{-s}\right) \\ &= \left(\sum_f |f|^{-s}\right)\left(\sum_f |f|^{-(s-1)}\right) \\ &= \frac{1}{(1-q^{1-s})(1-q^{1-(s-1)})} \\ &= \frac{1}{(1-q^{1-s})(1-q^{2-s})}\end{aligned}$$

□

Exercise 21. Let F be a field with $q = p^n$ elements. For $\alpha \in F$ set $f(x) = (x-\alpha)(x-\alpha^p)(x-\alpha^{p^2})\cdots(x-\alpha^{p^{n-1}})$. Show that $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$. In particular, $\alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}$ and $\alpha \cdot \alpha^p \cdots \alpha^{p^{n-1}}$ are in $\mathbb{Z}/p\mathbb{Z}$.

Proof. Consider the Frobenius automorphis $\tau : F \to F$ by sending $\tau(r) = r^p$ for each $r \in F$. It is a field automorphism since

1. $(r+s)^p = r^p \sum_{k=1}^{p-1} \binom{p}{k} r^{p-k}s^k + s^p = r^p + s^p$
2. $(rs)^p = r^p s^p$.
3. If $r^p = s^p$, then $(r-s)^p = r^p - s^p = 0$ (it works in charateristic 2, as $(r-s)^2 = r^2 + s^2 = r^2 - s^2$), thus $r = p$. In other words, τ is injective.
4. Since F is finite, an injective map is bijective.

We the lift τ to the polynomials, which should be a ring homomorphism. Note that the fixed points $r^p = r$ of F is exactly elements of the prime subfield $\mathbb{Z}/p\mathbb{Z}$, and so the polynomials fixed by τ is exactly the ones with coefficient in $\mathbb{Z}/p\mathbb{Z}$.

From there, we just need to note that

$$\begin{aligned}\tau(f(x)) &= (x-\alpha^p)(x-\alpha^{p^2})\cdots(x-\alpha^{p^{n-1}})(x-\alpha^{p^n}) \\ &= (x-\alpha^p)(x-\alpha^{p^2})\cdots(x-\alpha^{p^{n-1}})(x-\alpha) \\ &= f(x)\end{aligned}$$

□

Exercise 22 (continuation)**.** Set $\mathrm{tr}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}$. Prove that

1. $\mathrm{tr}(\alpha) + \mathrm{tr}(\beta) = \mathrm{tr}(\alpha + \beta)$.
2. $\mathrm{tr}(a\alpha) = a\,\mathrm{tr}(\alpha)$ for $a \in \mathbb{Z}/p\mathbb{Z}$.
3. There is an $\alpha \in F$ such that $\mathrm{tr}(\alpha) \neq 0$.

Proof.
Part 1: since we have shown $(\alpha + \beta)^p = \alpha^p + \beta^p$, we can prove that

$$(\alpha + \beta)^{p^k} = (\alpha^p + \beta^p)^{p^{k-1}} = (\alpha^{p^2} + \beta^{p^2})^{p^{k-2}} = \alpha^{p^k} + \beta^{p^k}$$

for any $k \geq 0$. Thus,

$$\begin{aligned}\mathrm{tr}(\alpha) + \mathrm{tr}(\beta) &= (\alpha + \beta) + (\alpha^p + \beta^p) + \cdots + (\alpha^{p^{n-1}} + \beta^{p^{n-1}}) \\ &= (\alpha + \beta) + (\alpha + \beta)^p + \cdots + (\alpha + \beta)^{p^{n-1}} \\ &= \mathrm{tr}(\alpha + \beta)\end{aligned}$$

Part 2: since $a^p = a$ for all $a \in \mathbb{Z}/p\mathbb{Z}$, we get

$$\mathrm{tr}(a\alpha) = a\alpha + a\alpha^p + \cdots + a\alpha^{p^{n-1}}) = a\,\mathrm{tr}(\alpha)$$

Part 3: if suppose $\mathrm{tr}(\alpha) = 0$ for all $\alpha \in F$, then the polynomial $x + x^p + \cdots + x^{p^{n-1}}$ has a total of p^n in F. However, the degree is less than p^n, a contradiction. $\square$

Exercise 23 (continuation)**.** For $\alpha \in F$ consider the polynomial $x^p - x - \alpha \in F[x]$. Show that this polynomial is either irreducible or the product of linear factors. Prove that the latter alternative holds iff $\mathrm{tr}(\alpha) = 0$.

Proof. Note that $(x+1)^p - (x+1) - \alpha = x^p + 1 - x - 1 - \alpha = x^p - x - \alpha$, so if it has a root in F, then it all of its roots are in F (by shifting a root).

Let K be the splitting field of the polynomial (possibly equal to F), and say $r \in K$ be one of its root. For each root $r + a$ ($a \in \mathbb{Z}/p\mathbb{Z}$), let $m_a(x)$ be its minimal (monic) polynomial. Since $m_a(x + a - b)$ has root $r + b$, we know that $\deg m_a(x) \leq \deg m_b(x)$. By symmetry, we must have $\deg m_a(x) = \deg m_b(x) = m$ for all $a, b \in \mathbb{Z}/p\mathbb{Z}$. On the other hand, by minimality, we know that $m_a(x) \mid x^p - x - \alpha$, so $x^p - x - \alpha$ is the product of *distinct* m_a. Suppose there are k such, then $p = km$. Hence, either

1. $m = 1$, which implies $x^p - x - a$ splits completely.
2. $m = p$, which implies $x^p - x - \alpha$ is irreducible (since a minimal polynomial is irreducible).

*Suppose $x^p - x - \alpha$ splits completely in $F[x]$. Equivalently, there exists some $r \in F$ such that $x^p - x - \alpha = (x - r)[x - (r+1)][x - (r+2)] \cdots [x - (r+p-1)]$. Consider the constant coefficient:

$$\mathrm{tr}(\alpha) = \sum_{k=0}^{n-1} (r^p - r)^{p^k} = \sum_{k=0}^{n-1} r^{p^{k+1}} - r^{p^k} = r^{p^n} - r = 0$$

Vice versa, suppose $x^p - x - \alpha$ is irreducible over F. This means that $r^p - r \neq \alpha$ for all $r \in F$. Since the Frobenius automorphism τ has $\mathbb{Z}/p\mathbb{Z}$ as its set of fixed point, $\tau - 1 : F \to F$ is a group homomorphism with kernel $\mathbb{Z}/p\mathbb{Z}$, thus its image $S = \{r^p - r : r \in F\}$ must have cardinality of p^{n-1} (using 1st isomorphism theorem).

On the other hand, we already prove that $\mathrm{tr}(\gamma) = 0$ for all $\gamma \in S$. So the elements of S should be roots of $x + x^p + \cdots + x^{p^{n-1}} = 0$. However, $|S| = p^{n-1}$, so S is exactly the set of roots of $x + x^p + \cdots + x^{p^{n-1}} = 0$. Equivalently, S is exactly the set of γ such that $\mathrm{tr}(\gamma) = 0$. Since $x^p - x - \alpha$ is irreducible, we have $\alpha \notin S$, and so $\mathrm{tr}(\alpha) \neq 0$. □

Exercise 24. Suppose that $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ has the property that $f(x+y) = f(x) + f(y) \in \mathbb{Z}/p\mathbb{Z}[x,y]$. Show that $f(x)$ must be of the form $a_0x + a_1x^p + a_2x^{p^2} + \cdots + a_mx^{p^m}$.

Proof. Using Lucas theorem, we know that, unless n is a power of p, then there is some $1 \leq k \leq n-1$ such that $\binom{n}{k} \not\equiv 0 \pmod{p}$. Indeed, if n is not a power of p, then either $a_r > 1$, or $a_i \neq 0$ for some $1 \leq i \leq r-1$ where $n = a_rp^r + \cdots + a_1p + a_0$ is the representation of n in base p.

1. If $a_r > 1$, pick $k = p^r < a_rp^r \leq n$. Then
$$\binom{n}{k} \equiv \binom{a_r}{1}\binom{a_{r-1}}{0}\binom{a_{r-2}}{0}\cdots\binom{a_0}{0} \equiv a_r \not\equiv 0 \pmod{p}$$
2. If $a_i \geq 1$ for some $1 \leq i \leq r-1$, pick $k = p^i \leq a_ip^i < a_ip^i + p^r \leq n$. Then
$$\binom{n}{k} \equiv \binom{a_r}{0}\cdots\binom{a_{i+1}}{0}\binom{a_i}{1}\binom{a_{i-1}}{0}\cdots\binom{a_0}{0} \equiv a_i \not\equiv 0 \pmod{p}$$

So if $f(x)$ contains some non-zero term a_nx^n such that n is not a power of p, then $f(x+y)$ has non-zero term $a_n\binom{n}{k}x^ky^{n-k}$ modulo p, while $f(x)+f(y)$ only has terms of the form x^i or y^j, a contradiction to the hypothesis. As for the constant term a_0, we have $a_0 = 2a_0$, so $a_0 = 0$. □