of cardinality k, there exists a permutation $\pi \in S_k$ such that the products $a_i b_{\pi(i)}$ are all distinct. Applying Lemma 9.18, it suffices to verify that the Vandermonde permanent $\mathrm{Per}_k(a_1, \ldots, a_k) = \sum_{\pi \in S_k} \prod_{i=1}^k a_i^{\pi(i)-1}$ is non-vanishing in $\mathbf{Q}(\omega)$. Note that each of the summands in this permanent is a qth root of unity, and the number $|S_k| = k!$ of summands is not divisible by p. The claim then follows from Lemma 9.49. □

Exercises

9.3.1 Show that Conjecture 9.15 fails whenever the ambient group Z has even order. (Hint: first consider the case $Z = \mathbf{Z}_2$.)

9.3.2 [67] Let p be a prime, let $1 \leq k < p$, and let F be a field of characteristic equal to p or zero. and let $a_1, \ldots, a_k \in F$. Then for any subset $B = \{b_1, \ldots, b_k\}$ of G, there is a permutation $\pi \in S_k$ such that the sums $a_1 + b_{\pi(1)}, a_2 + b_{\pi(2)}, \ldots, a_k + b_{\pi(k)}$ are all different. (By Exercise 9.4.4, this implies that Snevily's conjecture is true whenever G is the group $\mathbf{Z}_p^\alpha$ for any $\alpha \geq 0$.)

9.3.3 [67] Let $R \ni 1$ be a commutative ring, and let $\pi \in S_k$ be a permutation. Let $P_\pi \in R[u_1, \ldots, u_k, v_1, \ldots, v_k]$ to be the polynomial

$$P_\pi(u_1, \ldots, u_k; v_1, \ldots, v_k) := \prod_{1 \leq i < j \leq n} \big(u_j v_{\pi(j)} - u_i v_{\pi(i)}\big).$$

Verify the identity

$$\sum_{\pi \in S_k} P(\pi) = \Delta_k(u_1, \ldots, u_k)\mathrm{Per}_k(v_1, \ldots, v_k)$$

and use this to derive an alternative proof of Lemma 9.18.

9.4 Finite fields

We now pause to develop some of the theory of finite fields. We have already encountered the finite fields $F_p = \mathbf{Z}_p$ of prime order, but we now discuss more general finite fields of composite (prime power) order.

To avoid degeneracies we always assume that our fields have order at least 2 (so that $0 \neq 1$). Note that a finite field F is a finite additive group $(F, 0, +, -)$, but if one removes the 0 element one obtains a multiplicative group $(F^\times, 1, \times, \cdot^{-1})$, where $F^\times := F \backslash \{0\}$. Strictly speaking, a finite field has two multiplicative structures, the multiplicative group structure $x \times y$ for $x, y \in F$ and the $\mathbf{Z}$-module structure $n \cdot x$ for $n \in \mathbf{Z}, x \in F$ coming from iterated addition, but they are clearly related by the identity $n \cdot x = (n \cdot 1) \times x$; because of this, we shall abuse notation and identify n with $n \cdot 1$, and also identify the two multiplicative structures.

The most important examples of a finite field are the cyclic groups $F_p := \mathbf{Z}_p$ of prime order $|F_p| = p$. More generally, for any prime p and any integer $k \geq 1$, one can create a finite field F_{p^k} of order $|F_{p^k}| = p^k$ (Exercise 9.4.4). Such fields are unique up to field isomorphism (Exercise 9.4.6).

Because a finite field has both an additive and a multiplicative group structure, we will sometimes subscript certain group-theoretic concepts by addition or multiplication as appropriate. For instance, we use $\mathrm{ord}_+(x)$ to denote the additive order of $x \in F$ and $\mathrm{ord}_\times(x)$ to denote the multiplicative order. We now observe that all non-zero elements $x \in F^\times$ of a finite field have the same additive order $\mathrm{ord}_+(x)$.

Lemma 9.21 *Let F be a finite field, and let $p := \mathrm{ord}_+(1)$. Then p is prime, and $\mathrm{ord}_+(x) = p$ for all $x \in F^\times$.*

Proof If $\mathrm{ord}_+(1) = nm$ is composite for some $n, m > 1$, then $m \cdot 1, n \cdot 1 \neq 0$ but $(n \cdot 1) \times (m \cdot 1) = 0$, which contradicts the fact that $F^\times$ is a multiplicative group. Thus $\mathrm{ord}_+(1)$ is equal to a prime p. Since $p \cdot x = (p \cdot 1) \times x = 0 \times x = 0$, we see that $\mathrm{ord}_+(x)$ divides p for all $x \in F^\times$; since $\mathrm{ord}_+(x) \neq 1$, the claim follows. □

We call the prime $\mathrm{char}(F) := p = \mathrm{ord}_+(1)$ the *characteristic* of the finite field F. It is easy to see that F is now a vector space over F_p; in particular it has some dimension $k \geq 1$, and so $|F| = p^k$. From Cauchy's theorem (Exercise 3.1.2) applied to $F^\times$ we see that $\mathrm{ord}_\times(x)$ divides $|F^\times| = |F| - 1$ for all $x \in F^\times$. In other words,

$$x^{|F|-1} = 1 \text{ for all } x \in F^\times \tag{9.8}$$

and thus

$$x^{|F|} = x \text{ for all } x \in F. \tag{9.9}$$

This has the following consequence. For any positive integer n, define the *Euler totient function* $\phi(n)$ of n to be the number of elements in $[1, n]$ which are coprime to n (or equivalently, $\phi(n) = |\mathbf{Z}_n^\times|$).

Lemma 9.22 *Let F be a finite field, and let $n \geq 1$ be an integer dividing $|F^\times| = |F| - 1$. Then we have $|\{x \in F^\times : x^n = 1\}| = n$ and $|\{x \in F^\times : \mathrm{ord}_\times(x) = n\}| = \phi(n)$.*

Proof Since $x^n - 1$ has degree n, it has at most n zeroes, thus $|\{x \in F^\times : x^n = 1\}| \leq n$. On the other hand, if we write $|F| - 1 = nm$, we see from (9.8) that y^m lies in the set $\{x \in F^\times : x^n = 1\}$ for all $y \in F^\times$. Since the polynomial $y^m - c$ has at most m zeroes for each $c \in F$, we thus see that $|\{x \in F^\times : x^n = 1\}| \geq$

$|F^\times|/m = n$. This gives the first claim. This implies that

$$\begin{aligned}\sum_{d|n} |\{x \in F^\times : \mathrm{ord}_\times(x) = d\}| &= |\{x \in F^\times : x^n = 1\}| \\ &= n \\ &= \sum_{d|n} \phi(d)\end{aligned}$$

and the second claim now follows from an induction argument. □

Since $\phi(n) \neq 0$ for all $n \geq 1$, we thus see in particular that $F^\times$ contains an element of order $|F| - 1$; we call such elements *primitive elements* of $F^\times$. This implies in particular that $F^\times$ is a multiplicative cyclic group of order $|F| - 1$. Another consequence is

Lemma 9.23 *Let F be a finite field. Then for any $k \geq 1$ and any $h_1, \ldots, h_k \geq 0$ such that $\min(h_1, \ldots, h_k) < |F| - 1$, we have $\sum_{x_1,\ldots,x_k \in F} x_1^{h_1} \cdots x_k^{h_k} = 0$.*

Proof By factorizing the left-hand side, we see that it suffices to show that $\sum_{x \in F} x^h = 0$ for all $0 \leq h < |F| - 1$. When $h = 0$ we have $\sum_{x \in F} x^h = |F| \cdot 1 = 0$, since $|F|$ is a multiple of the characteristic $\mathrm{char}(F)$. Now suppose that $0 < h < |F| - 1$, and let ω be any primitive element of $F^\times$. Then $x \mapsto \omega x$ is a bijection on F, and so

$$\sum_{x \in F} x^h = \sum_{x \in F} (\omega x)^h = \omega^h \sum_{x \in F} x^h.$$

Since ω is primitive, $\omega^h \neq 1$, and hence $\sum_{x \in F} x^h = 0$ as claimed. □

We can now give the classical theorem of Chevalley and Warning on the number of solutions of a system of multi-variable polynomials over a finite field.

Theorem 9.24 (Chevalley–Warning theorem) *Let F be a finite field, let $n \geq 1$, and $P_1, \ldots, P_m \in F[t_1, \ldots, t_n]$ be polynomials such that $\sum_{i=1}^m \deg(P_i) < n$. Then the number of solutions $(x_1, \ldots, x_n) \in F^n$ to the equations*

$$P_1(x_1, \ldots, x_n) = \cdots = P_m(x_1, \ldots, x_n) = 0 \tag{9.10}$$

is a multiple of $\mathrm{char}(F)$.

Proof From (9.8) we have

$$\mathbf{I}(P_i(x_1, \ldots, x_n) = 0) = 1 - P_i(x_1, \ldots, x_n)^{|F|-1},$$

so the number of solutions to (9.10), thought of as an element of F, can be expressed as

$$\sum_{x_1,\ldots,x_n \in F} \prod_{i=1}^m \big(1 - P_i(x_1, \ldots, x_n)^{|F|-1}\big).$$

To prove the theorem, it thus suffices to show that

$$\sum_{x_1,\ldots,x_n \in F} \prod_{i=1}^{m} \left(1 - P_i(x_1, \ldots, x_n)^{|F|-1}\right) = 0. \tag{9.11}$$

By expanding the product $\prod_{i=1}^{m}(1 - P_i(x_1, \ldots, x_n)^{|F|-1})$ we get a linear combination of monomials of the form $\prod_{j=1}^{m} x_j^{a_j}$, each of which has degree at most $\sum_{i=1}^{m} \deg(F)(|F| - 1) < n(|F| - 1)$. By the pigeonhole principle this means that $\min(a_1, \ldots, a_m) < |F| - 1$, and thus by Lemma 9.23, each monomial gives a zero contribution to (9.11). The claim follows. □

Since $\mathrm{char}(F) \geq 2$, we have the following corollary:

Corollary 9.25 *Let $P_1, \ldots, P_m$ be as in Theorem 9.24. Then if there is one solution in F^n to (9.10), there must also exist at least one other solution.*

Next, we give a useful lemma which shows that the zeroes of sparse polynomials cannot have too high a multiplicity.

Lemma 9.26 *[180],[120] Let F be a finite field of prime order, and let $P \in F[t]$ be a non-zero polynomial of degree at most $|F| - 1$ with at most k non-zero coefficients. Then all the zeroes of P in $F^\times$ are of order at most $k - 1$; in other words, P does not contain any factors of the form $(x - x_0)^k$ for any $x_0 \in F^\times$.*

Proof We prove this by induction on k. The claim is trivial if $k = 1$, so suppose $k > 1$ and the claim has already been proven for $k - 1$. Suppose that the x^j coefficient of P was non-zero. If P contained a zero of order at least k in $F^\times$, the (formal) derivative P' must then contain a zero of order at least $k - 1$, and so $xP' - jP$ must also contain a zero of order at least $k - 1$. But $xP' - jP$ is a non-trivial polynomial with at most $k - 1$ non-zero coefficients, contradicting the induction hypothesis. Thus all the zeroes of P in $F^\times$ are of order at most $k - 1$. □

Exercises

9.4.1 Let R be a commutative ring containing 1, and let $R[t]^{\mathrm{monic}}$ be the multiplicative semigroup of all monic polynomials in $R[t]$ (polynomials with leading coefficient 1). We say that a monic polynomial is irreducible if it has no proper monic factors. Using the Euclidean algorithm, show that every monic polynomial can be uniquely factored into monic irreducible factors, up to permutations. In particular this shows that $F[t]$ is a unique factorization domain whenever F is a field.

9.4.2 Let F be a finite field. Define the *von Mangoldt function* $\Lambda : F[t]^{\mathrm{monic}} \to \mathbf{R}$ by setting $\Lambda(f) := \deg(g)$ if $f = g^k$ for some irreducible g and

some $k \geq 1$, and $\Lambda(f) := 0$ otherwise. Using Exercise 9.4.1, show that $\deg(f) := \sum_{g \in F[t]^{\text{monic}}; g|f} \Lambda(g)$ for all $f \in F[t]^{\text{monic}}$, where we use $g|f$ to denote that g is a factor of f. Conclude in particular

$$\sum_{f \in F[t]^{\text{monic}}} \frac{\deg(f)}{|F|^{s \deg(f)}} = \left(\sum_{f \in F[t]^{\text{monic}}} \frac{\Lambda(f)}{|F|^{s \deg(f)}} \right) \sum_{f \in F[t]^{\text{monic}}} \frac{1}{|F|^{s \deg(f)}}$$

for all $s > 1$. From this, conclude the *prime number theorem* for $F[t]$:

$$\sum_{f \in F[t]^{\text{monic}}; \deg(f) = k} \Lambda(f) = |F|^k \text{ for all } k \geq 1.$$

From this, conclude *Bertrand's postulate* for $F[t]$: for every $k \geq 1$ there exists at least one irreducible monic polynomial in $F[t]^{\text{monic}}$ of degree k. Also, establish the *Riemann hypothesis* for $F[t]$:

$$|\{f \in F[t]^{\text{monic}} : \deg(f) = k, f \text{ irreducible}\}| = |F|^k/k + O\big(|F|^{k/2}\big).$$

Note that this is considerably easier to establish than the corresponding Riemann hypothesis for $\mathbf{Z}$!

9.4.3 Let F be a finite field of order $|F| = p^k$ for some prime p and some $k \geq 1$. Let $f(t) \in F_p[t]$ be a polynomial over F_p such that $f(t) | t^{p^k} - t$. Show that $f(t)$ has exactly $\deg(f)$ distinct zeroes in F. (Hint: if $t^{p^k} - t = f(t)g(t)$, the zeroes of $t^{p^k} - t$ are the union of the zeroes of $f(t)$ and the zeroes of $g(t)$.) In the language of Galois theory, this means that every factor of $t^{p^k} - t$ splits completely over F.

9.4.4 Let F be a finite field and $k \geq 1$ be an integer. Let $f(t) \in F[t]$ be a monic irreducible polynomial of degree k (which exists by Exercise 9.4.2). Show that the quotient ring $F[t]/(f(t))$ is a finite field of order $|F|^k$. Show that this finite field is isomorphic *as an additive group only* to the vector space F^k. Note that this construction shows that there exists a field of order p^k for any prime p and any $k \geq 1$.

9.4.5 Let F be a finite field of order $|F| = p^k$ for some prime p and some $k \geq 1$. Let ω be a primitive element of $F^\times$. Let $f(t) \in F_p[t]$ be the minimal polynomial of ω over F_p, i.e. the monic polynomial in $F_p[t]$ of minimal degree such that $f(\omega) = 0$. Show that $\deg(f) = k$, and that the vectors $1, \omega, \ldots, \omega^{k-1}$ form a basis for F, viewed as a vector space over F_p.

9.4.6 Let F and G be two finite fields of the same order $|F| = |G| = p^k$. Prove that F and G are isomorphic. (Hint: let ω be a primitive element of $F^\times$, and let $f(t)$ be the minimal polynomial of ω. Use Exercise 9.4.3 to find