$\omega' \in G^\times$ such that $f(\omega') = 0$, and then find a field isomorphism between F and G which maps ω to ω'.)

9.4.7 Let $F = F_{p^k}$ be a finite field of characteristic p, and let $\phi : F \to F$ be the *Frobenius map* $\phi(x) := x^p$. Show that ϕ is a field isomorphism. Furthermore, show that the iterates $\phi^0, \phi^1, \ldots, \phi^{k-1}$ of this map are the only field isomorphisms of F to itself.

9.4.8 Let $F = F_{p^k}$ be a finite field, and let $1 \leq k' \leq k$. Show that the set $G := \{x \in F : x^{p^{k'}} = x\}$ is a subfield of F of order $|G| = |p^{k'}|$.

9.4.9 (Wilson's theorem) If p is a prime, show that $(p-1)! \cdot 1 = -1$ in F_p. (Hint: show that if $x \in F_p^\times$, then $x = x^{-1}$ if and only if $x = \pm 1$.)

9.4.10 Show that Lemma 9.26 fails when F is not of prime order. (Hint: if $|F| = p^k$, consider the polynomial $x^p - x$.)

9.4.11 Use Corollary 9.25 to give an alternative proof of Exercise 4.3.16 which does not use the Fourier transform.

9.5 Davenport's problem

For an finite additive group Z, define the *Davenport number* $s = s(Z)$ of Z to be the smallest integer such that whenever $a_1, \ldots, a_s$ are elements of Z (not necessarily distinct), there exists a partial sum $\sum_{i \in I} a_i$ of the a_i for some non-empty $I \subseteq [1, s]$ which sums to zero. The problem of determining $s(Z)$ for arbitrary groups Z was posed by Davenport in 1966. A simple estimate is

Lemma 9.27 *If Z is a finite additive group, then $s(|Z|) \leq |Z|$.*

Proof Let $a_1, \ldots, a_{|Z|}$ be elements of Z; it suffices to show that some non-trivial partial sum of these elements is zero. Consider the $|Z|$ partial sums $a_1, a_1 + a_2, \ldots, a_1 + \cdots + a_{|Z|}$. If one of them is zero, we are done. Otherwise, by the pigeonhole principle there exists two such partial sums which are equal. Subtracting the shorter partial sum from the longer, we obtain the result. □

In 1961, Erdős, Ginzburg and Ziv [88] proved the following remarkable variant.

Theorem 9.28 *[88] Let Z be a finite additive group, and $a_1, \ldots, a_{2|Z|-1}$ be elements of $|Z|$. Then there exists $I \subset [1, 2|Z| - 1]$ with $|I| = |Z|$ such that $\sum_{i \in I} a_i = 0$.*

Proof Let us start with the special case when $Z = \mathbf{Z}_p$ is a cyclic group of prime order. In this case we use Chavelley–Warning theorem to derive the claim. Let

$F = F_p = \mathbf{Z}_p$ and let $P_1, P_2 \in F[t_1, \ldots, t_{2p-1}]$ be the polynomials

$$P_1(t_1, \ldots, t_{2p-1}) = \sum_{i=1}^{2p-1} a_i t_i^{p-1}; \quad P_2(t_1, \ldots, t_{2p-1}) = \sum_{i=1}^{2p-1} x_i^{p-1}.$$

Observe that $\deg(P_1) + \deg(P_2) = 2(p-1) < 2p-1$, and that $(0, \ldots, 0)$ is a simultaneous root of P_1 and P_2, and hence by Corollary 9.25 we can find another simultaneous root $(y_1, \ldots, y_{2p-1}) \neq 0$ of P_1 and P_2. But by (9.8) we see that $\sum_{i=1}^{2p-1} y_i^{p-1} := |\{i \in [1, 2p-1] : y_i \neq 0\}| \cdot 1$. The claim then follows by setting $I := \{i \in [1, 2p-1] : y_i \neq 0\}$.

In the general case, we induce on $|Z|$. If $|Z|$ is prime then we are already done, so suppose that $|Z| = pm$ for some prime p and some $1 \leq m < |Z|$. Then (using Corollary 3.8 if necessary) we can find a surjective homomorphism $\phi : Z \to \mathbf{Z}_p$ whose kernel $G := \ker(\phi)$ is a subgroup of Z of order m. Since we have already proven the theorem for $\mathbf{Z}_p$, we see that for any sequence of $2p-1$ elements of Z, we can already obtain a subsequence of size p which lies in G. By the greedy algorithm, we can thus locate $2m-1$ disjoint subsets $I_1, \ldots, I_{2m-1}$ of cardinality p inside $[1, 2|Z|-1]$ such that $\sum_{i \in I_j} a_i \in G$ for each $1 \leq j \leq 2m-1$. Now write $\sum_{i \in I_j} a_i = b_j$. By induction hypothesis we can find a subset $J \subset [1, 2m-1]$ of cardinality m such that $\sum_{j \in J} b_j = 0$. The claim now follows by setting $I := \bigcup_{j \in J} I_j$. □

From considering the sequence $1, \ldots, 1$ and Lemma 9.27 we see that $s(\mathbf{Z}_p) = p$ for any prime p, and more generally that

$$s(\mathbf{Z}_{p^{k_1}} \oplus \cdots \oplus \mathbf{Z}_{p^{k_l}}) \geq 1 + \sum_{i=1}^{l} (p^{k_i} - 1) \tag{9.12}$$

for any prime p and any $k_1, \ldots, k_l \geq 1$ (see Exercise 9.5.1).

Olson [266] proved that this bound is sharp. Let us first see this in the case $k_1 = \cdots = k_l = 1$, by modifying the proof of Theorem 9.28.

Proposition 9.29 *For any $l \geq 1$ and any prime p, we have $s(\mathbf{Z}_p^l) = 1 + l(p-1)$.*

Proof By (9.12) it suffices to prove the upper bound. Write $F := \mathbf{Z}_p$. Consider a sequence $a_1, \ldots, a_n \in F^l$ where $n \geq 1 + l(p-1)$. Each a_i can be viewed as an l-dimensional vector and we write $a_i = (a_{i1}, \ldots, a_{il})$. Let $P_1, \ldots, P_l \in F[t_1, \ldots, t_n]$ be the polynomials $P_j(t_1, \ldots, t_n) := \sum_{i=1}^{n} a_{ij} t_i^{p-1}$ for $1 \leq j \leq l$; then $\sum_{j=1}^{l} \deg(P_j) = l(p-1) < n$. Since $(0, \ldots, 0)$ is a simultaneous zero of $P_1, \ldots, P_l$, we thus see from Corollary 9.25 that there must exist another simultaneous zero $(y_1, \ldots, y_n) \neq (0, \ldots, 0)$. Setting $I := \{i \in [1, n] : y_i \neq 0\}$, we conclude using (9.8) as before that $\sum_{i \in I} a_i = 0$, as desired. □

This simple argument does not directly extend to the general groups considered in (9.12); nevertheless, Olson was able to proceed by a different argument.

Theorem 9.30 *[266] Let p be a prime and $k_1, \dots, k_l \geq 1$. Then the inequality (9.12) in fact holds with equality.*

Proof Again it suffices to prove the upper bound. It is convenient to use multiplicative notation. Let G be an abelian multiplicative group which is isomorphic to the additive group $\mathbf{Z}_{p^{k_1}} \oplus \cdots \oplus \mathbf{Z}_{p^{k_l}}$, let $n \geq 1 + \sum_{i=1}^{l}(p^{k_i} - 1)$, and let $g_1, \dots, g_n \in G$. It will suffice to find $I \in [1, n]$ such that $\prod_{i \in I} g_i = 1$.

Let R be the group ring of G over $\mathbf{Z}_p$ (i.e. R is the space of formal linear combinations of elements of G with coefficients in $\mathbf{Z}_p$). In this ring we claim that

$$(1 - g_1) \cdots (1 - g_n) = 0.$$

To see this, let $x_1, \dots, x_l$ be the standard basis for G, where x_i has order p^{k_i}. Each g_j can be written as the product of a few x_is. We use the identity $1 - xy = (1 - x) + x(1 - y)$ iteratively to replace $1 - g_j$ as a linear combination (with coefficient in R) of the elements $1 - x_i$. Thus, it follows that the product $(1 - g_1) \cdots (1 - g_n)$ is a linear combination of elements of the form $\prod_{i=1}^{l}(1 - x_i)^{n_i}$ where $\sum_{i=1}^{l} n_i = n > \sum_{i=1}^{l}(p^{k_i} - 1)$. There must be some j such that $n_j \geq p^{k_j}$. On the other hand, in R, $(1 - x_j)^{p^{k_j}} = 1 - x_j^{p^{k_j}} = 0$. It follows that $(1 - g_1) \cdots (1 - g_n) = 0$, as claimed. This implies that for some non-trivial subsequence of the g_i has product 1, because otherwise, the coefficient of 1 in the product $(1 - g_1) \cdots (1 - g_n)$ would be non-zero. This proves Theorem 9.30. □

This allows us to prove variants of Theorem 9.28 for product groups. For instance:

Lemma 9.31 *[266] Let $Z := \mathbf{Z}_p^2$ where p is a prime. For any sequence $a_1, \dots, a_{3p-2} \in Z$, one can find a subsequence of length at most p whose sum is zero.*

Proof Embed Z in $Z' := \mathbf{Z}_p^3$ and a sequence $x + a_1, \dots, x + a_{3p-2}$, where x is an element of $Z' \backslash Z$. By Theorem 9.30 (or Proposition 9.29) we have $s(Z') = 3p - 3$, and thus some subsequence of $x + a_1, \dots, x + a_{3p-3}$ has sum zero. Rearranging subscripts, we may assume that $(x + a_1) + \cdots + (x + a_n) = 0$, where $1 \leq n \leq 3p - 3$. This implies that $nx = 0$ and $g_1 + \cdots + g_n = 0$. It follows that $n = p$ or $n = 2p$. If $n = p$ then we are done. If $n = 2p$, we apply Theorem 9.30 or Proposition 9.29 again, this time to the group Z. As $s(Z) = 2(p - 1)$, the sequence $a_1, \dots, a_{n-1}$ contains a subsequence whose sum is zero. Again by rearranging subscripts, we may assume that $g_1 + \cdots + g_m = 0$ where $m \leq n - 1$. If $m \leq p$

then we are done. If $m > p$, then the sequence $g_{m+1}, \ldots, g_m$ has length less than p and its sum is also zero since $g_1 + \cdots + g_n = 0$. The proof is complete. □

By this Lemma and an induction argument similar to that used to prove Theorem 9.28 one can then obtain the following estimate on the Davenport number of product groups:

Theorem 9.32 *[266] Let Z and W be additive groups such that $|W|$ divides $|Z|$. Then $s(Z \oplus W) \leq |Z| + |W| - 1$.*

We leave the proof of this theorem to Exercise 9.5.2.

Finally, let us briefly discuss the version of Davenport's problem when the elements in the sequence are different. Under this condition, the magnitude of the Davenport number changes dramatically. Szemerédi [347] proved

Theorem 9.33 *There is a constant c such that the following holds. Let $S = \{a_1, \ldots, a_s\}$ be a sequence of s different elements of $\mathbf{Z}_p$, where p is a prime and $s > c\sqrt{p}$. Then there is a non-empty subsequence of S whose elements sum up to zero.*

A more recent result of Hamidoune and Zemor [175] showed that one can set $c = \sqrt{2} + o(1)$, which is asymptocially best possible.

Assume that $A \subset \mathbf{Z}_p$ does not contain 0 and view the elements of A as integers between 1 and $p - 1$. It is clear that if $\sum_{a \in A} a < p$ then no subset of A sums up to 0. In [349, 352], Szemerédi and Vu showed that if A has sufficiently many elements, then this is essentially the only reason.

Theorem 9.34 *Let A be a subset of $\mathbf{Z}_p$, where p is a large prime. Assume that no subset of A sums up to 0. Then there is a subset A' of A with at most $p^{0.49}$ elements and a non-zero element $x \in \mathbf{Z}_p$ such that the sum of the elements in $x \cdot (A \backslash A')$ (viewed as positive integers between 1 and $p - 1$) is less than p.*

For another classification result of this kind, see Theorem 12.20. The approach to these two results relies on inverse arguments, in spirit of those discussed in Chapter 12.

Exercises

9.5.1 Prove (9.12).

9.5.2 By modifying the inductive argument in the proof of Theorem 9.28, deduce Theorem 9.32 from Lemma 9.31.

9.5.3 Let n be a positive integer, and let $\mathbf{Z}[i]$ be the ring of Gaussian integers. Show that a sequence of $2n - 1$ Gaussian integers contains a subsequence of length n whose sum is divisible by n.