cannot have certain types of zeroes if some combination of its coefficients are divisible (or not divisible) by p in a certain manner; the most well known example of this is Eisenstein's criterion (Exercise 9.8.2), but the combinatorial Nullstellensatz can also be viewed as a statement of this type, and another example arises in cyclotomic fields (Lemma 9.49). As an application of these criteria we present an uncertainty principle for $\mathbf{Z}_p$ which gives a Fourier-analytic proof of the Cauchy–Davenport inequality (Theorem 5.4).

Much of the theory pertains to arbitrary fields F. However, we will at times need to focus on two special types of fields. The first are *finite fields*, of which the primary example are the fields $F_p = \mathbf{Z}_p$ of prime order. We shall review the theory of these fields in Section 9.4. The second are the *cyclotomic fields*, generated by pth roots of unity; we shall review the theory of those fields in Section 9.8.

It is easy to see that in a field F, all non-zero elements have the same torsion as the identity element 1. We refer to this torsion as the *characteristic* $\mathrm{char}(F)$ of F; it is either zero (if F is torsion-free) or a prime p (which is for instance the case when F is finite). Some of our results will only hold if the characteristic of F is sufficiently large (or equal to zero).

9.1 The combinatorial Nullstellensatz

As is well known, a polynomial $P \in F[t]$ of one variable over a field F can have at most $\deg(P)$ zeroes, where $\deg(P)$ denotes the degree of P. Let us rewrite this fact as

Lemma 9.1 *Let $P \in F[t]$ be a polynomial of one variable over a field F and degree d (thus the t^d coefficient of P is non-zero) and let S be a subset of F such that $|S| > \deg(P)$. Then there exists $x \in S$ such that $P(x) \neq 0$.*

We now present a powerful generalization of this fact to polynomials of several variables, namely the *combinatorial Nullstellensatz* of Alon [4].

Theorem 9.2 (Combinatorial Nullstellensatz) *[4] Let F be an arbitrary field, let $P \in F[t_1, \ldots, t_n]$ be a polynomial of degree d which contains a non-zero coefficient at $t_1^{d_1} \cdots t_n^{d_n}$ with $d_1 + \cdots + d_n = d$, and let $S_1, \ldots, S_n$ be subsets of F such that $|S_i| > d_i$ for all $1 \leq i \leq n$. Then there exists $x_1 \in S_1, \ldots, x_n \in S_n$ such that $P(x_1, \ldots, x_n) \neq 0$.*

Proof We induce on n. The case $n = 1$ is just Lemma 9.1. Now suppose that $n \geq 2$ and the claim has already been proven for $n - 1$.

Let $g_n(t_n)$ be the polynomial of one variable

$$g_n(t_n) = \prod_{s_n \in S_n} (t_n - s_n) = t_n^{|S_n|} + \text{ lower order terms.}$$

Thus g_n has degree $|S_n|$ and the leading term is monic (i.e. it has coefficient 1). By applying the long division algorithm to P, we may write

$$P(t_1, \ldots, t_n) = q_n(t_1, \ldots, t_n) g_n(t_n) + r_n(t_1, \ldots, t_n)$$

where the quotient q_n is a polynomial of degree at most $d - |S_n|$, and the remainder r_n is a polynomial of degree at most d such that no monomial contains a factor of $t_n^{|S_n|}$, thus

$$r_n(t_1, \ldots, t_n) = \sum_{j=0}^{|S_n|} r_{n,j}(t_1, \ldots, t_{n-1}) t_n^j.$$

We can expand $q_n g_n$ as $q_n t_n^{|S_n|}$ plus lower-order terms, of degree at most

$$\deg(q_n) + |S_n| - 1 \leq (d - |S_n|) + |S_n| - 1 < d = d_1 + \cdots + d_n.$$

Thus the lower-order terms have a vanishing $t_1^{d_1} \cdots t_n^{d_n}$ coefficient. Since $|S_n| > d_n$, we see that $q_n t_n^{|S_n|}$ also has a vanishing $t_1^{d_1} \cdots t_n^{d_n}$ coefficient. Thus by hypothesis on P, the remainder r_n must have a non-zero $t_1^{d_1} \cdots t_n^{d_n}$ coefficient. In particular, r_{n,d_n} contains a non-zero $t_1^{d_1} \cdots t_{n-1}^{d_n - 1}$ coefficient. Applying the induction hypothesis, we can find $x_1 \in S_1, \ldots, x_{n-1} \in S_{n-1}$ such that $r_{n,d_n}(x_1, \ldots, x_{n-1})$ is non-zero. Applying Lemma 9.1, we can then find $x_n \in S_n$ such that

$$r_n(x_1, \ldots, x_n) = \sum_{j=0}^{|S_n|} r_{n,j}(x_1, \ldots, x_{n-1}) x_n^j \neq 0.$$

Since $g_n(x_n) = 0$, we thus have $P(x_1, \ldots, x_n) \neq 0$, as desired. □

For an explanation as to the terminology "combinatorial Nullstellensatz", see Exercise 9.1.3. Based on the Combinatorial Nullstelensatz, Alon, Nathanson and Ruzsa developed the so-called *polynomial method*, which is a very powerful tool for proving bounds concerning cardinalities of sum sets. The next several sections contain various applications of this method.

Exercises

9.1.1 (Schwartz–Zippel lemma) Let F be a field, let $Q \in F[t_1, \ldots, t_n]$ be a non-zero polynomial of $n \geq 1$ variables, and let S be a non-empty finite subset of F. Let $x_1, \ldots, x_n$ be elements of S chosen independently at random. Then

$$\mathbf{P}(Q(x_1, \ldots, x_n) = 0) \leq \frac{\deg(Q)}{|S|}.$$

(Hint: modify the induction argument used to prove the Nullstellensatz.)

9.1.2 Let F be a field, let $d_1, \ldots, d_n \geq 0$, and let $P \in F[t_1, \ldots, t_n]$ be a non-zero polynomial such that every monomial that occurs in P divides $t_1^{d_1} t_2^{d_2} \cdots t_n^{d_n}$. Show that there exist functions $f_{i,1}, \ldots, f_{i,d_i} : F^{i-1} \to F$ for each $1 \leq i \leq n$ such that

$$\{(x_1, \ldots, x_n) \in F^n : P(x_1, \ldots, x_n) = 0\}$$
$$\subseteq \bigcup_{i=1}^{n} \bigcup_{j=1}^{d_j} \{(x_1, \ldots, x_n) \in F^n : x_i = f_{i,j}(x_1, \ldots, x_{i-1})\};$$

thus the zero locus of P can be covered by a small number of graphs. Note that when $i = 1$ the functions $f_{1,j}$ are simply constants. Conclude in particular that the combinatorial Nullstellensatz holds for this choice of P and $d_1, \ldots, d_n$.

9.1.3 [4] Let F be an arbitrary field and $P \in F[t_1, \ldots, t_n]$ be a polynomial. Let $S_1, \ldots, S_n$ be non-empty subsets of F and let $g_1, \ldots, g_n \in F[t_1, \ldots, t_n]$ be the polynomials defined by $g_i(t_1, \ldots, t_n) := \prod_{s \in S_i} (t_i - s)$ for each $1 \leq i \leq n$. If P vanishes on $S_1 \times \cdots \times S_n$, show that there are polynomials $h_1, \ldots, h_n \in F[t_1, \ldots, t_n]$ satisfying $\deg h_i \leq \deg P - \deg g_i$ so that

$$P = \sum_{i=1}^{n} h_i g_i.$$

Moreover, the coefficients of $h_1, \ldots, h_n$ can be chosen to lie in the ring generated by the coefficients of P and $g_1, \ldots, g_n$. Use this and the previous exercise to provide an alternative proof of Theorem 9.2. This should be contrasted with the *Hilbert Nullstellensatz*, which asserts that given arbitrary polynomials $P, g_1, \ldots, g_n \in F[t_1, \ldots, t_n]$, with P vanishing on the algebraic variety determined by $g_1, \ldots, g_n$, then some power P^K of P can be written as a linear combination $P^K = \sum_{i=1}^{n} h_i g_i$ of $g_1, \ldots, g_n$.

9.1.4 Let $d_1, \ldots, d_n \geq 0$ be integers, and let F be a field whose characteristic is either zero or is greater than $\max(d_1, \ldots, d_n)$. Let $P \in F[t_1, \ldots, t_n]$ be such that the $t_1^{d_1} \cdots t_n^{d_n}$ coefficient is non-zero, but that no other non-zero monomial in P is divisible by $t_1^{d_1} \cdots t_n^{d_n}$. Let $S_1, \ldots, S_n \subset F$ be such that $|S_i| > d_i$ for all $1 \leq i \leq n$. Show that there exist $x_1 \in S_1, \ldots, x_n \in S_n$ such that $P(x_1, \ldots, x_n) = 0$. (Hint: for each $1 \leq i \leq n$, construct a function $g_i : S_i \to F$ such that $\sum_{x_i \in S_i} g_i(x_i) x_i^j = \mathbf{I}(j = d_i)$ for all $0 \leq j \leq d_i$. Then consider the quantity $\sum_{x_1 \in S_1, \ldots, x_n \in S_n} P(x_1, \ldots, x_n) g_1(x_1) \ldots g_n(x_n)$.)

9.1.5 Let F be a field and m a positive integer. Let $F^{\{0,1\}^m}$ be the ring of functions from $\{0, 1\}^m$ to F, and for each $i \in [1, m]$ let $x_i \in F^{\{0,1\}^m}$ be