UCD Mathematics Enrichment Programme 2017

Saturday March 25 2017

T. J. Laffey

Polynomial algebra, factorization and related number theory.

An expression of the form

$$f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n$$

is called a polynomial. Here $a_0, a_1, \cdots, a_n$ are numbers (usually real or complex numbers) and x is an <u>indeterminate</u> or <u>symbol</u>. If $a_0 \neq 0$, n is the <u>degree</u> of $f(x)$. One adds polynomials in the obvious way. If

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n,$$

$$g(x) = b_0x^n + b_1x^{n-1} + \cdots + b_n,$$

then $f(x)+g(x) = (a_0+b_0)x^n + (a_1+b_1)x^{n-1} + \cdots + (a_n+b_n)$.

For example $(4x^3 - 6x^2 + x + 1) + (-2x^2 + 3x - 3)$

$$= 4x^3 - 8x^2 + 4x - 2.$$

One multiplies polynomials in the usual way: multiply out the product of $f(x)\,g(x)$ fully and collect terms with the same power of x.

For example

$$(3x^2 - x + 4)(-4x^3 + x + 7) =$$

$$-12x^5 + 3x^3 + 21x^2 + 4x^4 - x^2 - 7x - 16x^3 + 4x + 28$$

$$= -12x^5 + 4x^4 - 13x^3 + 20x^2 - 3x + 28.$$

For $f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$,

$g(x) = b_0 x^m + b_1 x^{m-1} + \cdots + b_m$,

Then $f(x) g(x) = c_0 x^{n+m} + c_1 x^{n+m-1} + \cdots + c_r x^{n+m-r} + \cdots + c_{n+m}$,

where $c_0 = a_0 b_0$, $c_1 = a_0 b_1 + a_1 b_0$, $\ldots$,

$c_r = a_0 b_r + a_1 b_{r-1} + a_2 b_{r-2} + \cdots + a_r b_0$, $\ldots$,

$c_{n+m} = a_n b_m$.

Observe that the degree of $f(x) + g(x)$ $\leq$ maximum of degree $f(x)$, degree $g(x)$.

[Example ① $f(x) = 43x^2 - 7x + 2$, $g(x) = -x^3 + 1$,
degree$(f(x) + g(x)) = 3$,
② $f(x) = 3x^2 - 7x + 12$, $g(x) = x^2 + 1$,
degree$(f(x) + g(x)) = 2$,
③ $f(x) = 3x^2 - 7x + 2$, $g(x) = -3x^2 + 1$,
degree$(f(x) + g(x)) = 1$.]

Exercise: If $f(x)$ and $g(x)$ are nonzero polynomials, then degree$(f(x) g(x))$ = degree $f(x)$ + degree $g(x)$.

If $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$, then a_i is called the coefficient of x^{n-i}.

Example ① If $f(x) = 4x^2 - 7x + 11$, then the coefficient of x^2 is 4, -7 is the coefficient of x and 11 is the coefficient of x^0; 11 is also called the constant term.

② If $f(x) = 2x^3 - 1$, then the coefficient of x^2 is 0 and the coefficient of x is 0.

The zero polynomial has all its coefficients equal to 0.

One can add, subtract and multiply polynomials. One can also multiply a polynomial by a constant, for example $7(3x^2 - 6x + 1) = 21x^2 - 42x + 7$.

One can also perform long division on polynomials. If $f(x)$, $g(x)$ are polynomials and $g(x) \neq 0$, we can calculate polynomials $q(x)$, $r(x)$ such that

$$f(x) = g(x)q(x) + r(x)$$

where $r(x) = 0$ or degree $r(x) <$ degree$(g(x))$.

$q(x)$ is called the <u>quotient</u> and $r(x)$ the <u>remainder</u> on the division of $f(x)$ by $g(x)$.

We say that $g(x)$ <u>divides</u> $f(x)$ if the remainder $r(x) = 0$.

We say that α is a <u>zero</u> or <u>root</u> of $f(x)$ (or ~~of~~ $f(x) = 0$) if $f(\alpha) = 0$.

Given a polynomial $f(x)$ and a number β, we can perform a long division of $f(x)$ by $x - \beta$ to get

$$f(x) = (x-\beta)\, q(x) + r,$$

and note that $f(\beta) = 0$ <u>if and only if</u> the remainder $r = 0$.

This fact is called the <u>remainder theorem</u>.

$q(x)$ is called the <u>quotient</u> and $r(x)$ the <u>remainder</u> on the division of $f(x)$ by $g(x)$.

We say that $g(x)$ <u>divides</u> $f(x)$ if the remainder $r(x) = 0$.

We say that α is a <u>zero</u> or <u>root</u> of $f(x)$ (or ~~of~~ $f(x) = 0$) if $f(\alpha) = 0$.

Given a polynomial $f(x)$ and a number β, we can perform a long division of $f(x)$ by $x - \beta$ to get

$$f(x) = (x-\beta)\, q(x) + r,$$

and note that $f(\beta) = 0$ <u>if and only if</u> the remainder $r = 0$.

This fact is called the <u>remainder theorem</u>.

Suppose that $f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$ is a polynomial with $a_0, a_1, \cdots, a_n$ complex numbers and $a_0 \neq 0$. Then, if $n \geq 1$, there exist complex numbers $\alpha_1, \cdots, \alpha_n$ such that $f(x) = a_0 (x-\alpha_1)(x-\alpha_2) \cdots (x-\alpha_n)$ (1)

Furthermore, if $f(x) = a_0 (x-\beta_1)(x-\beta_2) \cdots (x-\beta_n)$, for some complex numbers $\beta_1, \beta_2, \cdots, \beta_n$, then the list $(\beta_1, \beta_2, \cdots, \beta_n)$ and (2) the list $(\alpha_1, \alpha_2, \cdots, \alpha_n)$ must be the same up to a permutation of their entries.

To prove this factorization exists, as a <u>first step</u>, we must show that there exists a complex number, γ say, with $f(\gamma) = 0$. One can then take $\alpha_1 = \gamma$ and write $f(x) = (x-\alpha_1)\, g(x)$, where $g(x) = a_0 x^{n-1} + b_1 x^{n-2} + \cdots + b_{n-1}$, for complex numbers $b_1, \cdots, b_{n-1}$. Using a proof by induction on the degree of the polynomial, we can assume that $n > 1$ and that the result holds for $g(x)$, since $g(x)$ has degree $n-1$.

So we can write

$$g(x) = a_0 (x-\alpha_2) \cdots (x-\alpha_n)$$

for some complex numbers $\alpha_2, \cdots, \alpha_n$ and

then
$$f(x) = (x-\alpha_1) g(x)$$
$$= a_0 (x-\alpha_1)(x-\alpha_2) \cdots (x-\alpha_n),$$

as claimed in (1) above.

If $f(\delta) = 0$ for some complex number δ, then

$$0 = a_0 (\delta - \alpha_1)(\delta-\alpha_2) \cdots (\delta - \alpha_n),$$

so, since $a_0 \neq 0$, $\delta - \alpha_j = 0$ for some j. In particular, if

$$f(x) = a_0 (x-\alpha_1)(x-\alpha_2) \cdots (x-\alpha_n)$$
$$= a_0 (x-\beta_1)(x-\beta_2) \cdots (x-\beta_n),$$

it follows from $f(\beta_1) = 0$, that $\beta_1 = \alpha_j$ for some j and then

$$a_0 (x-\alpha_1) \cdots (x-\alpha_{j-1})(x-\alpha_j)(x-\alpha_{j+1}) \cdots (x-\alpha_n)$$
$$= a_0 (x-\alpha_j)(x-\beta_2) \cdots\cdots (x-\beta_n)$$

and cancelling the factor $x-\alpha_j$ on both sides, we get

$$a_0(x-\alpha_1)\cdots(x-\alpha_{j-1})(x-\alpha_{j+1})\cdots(x-\alpha_n)$$
$$= a_0(x-\beta_2)(x-\beta_3)\cdots(x-\beta_n)$$

and using induction on n, we can assume that the list $(\beta_2, \beta_3, \cdots, \beta_n)$ must be a permutation of the list

$$(\alpha_1, \alpha_2, \cdots, \alpha_{j-1}, \alpha_{j+1}, \cdots, \alpha_n)$$

and then (2) follows.

So to prove the statements (1) and (2), it remains to establish the first step: namely, we must show that there exists a complex number γ with $f(\gamma) = 0$. This result may be stated formally as follows:

Fundamental Theorem of Algebra.

Let $f(x)$ be a polynomial with complex coefficients and degree at least one. Then there exists a complex number γ with $f(\gamma) = 0$.

While this result was believed to be true since the early 1600s, and several proofs were offered, errors were found in them very quickly. The first proof to survive criticism when it was published was by Carl Friedrich Gauss in Göttingen in 1799. However, in 1920, a gap was found in his proof and it was fixed by Alexander Ostrowski, who was born in Kiev, then in the Russian empire, and did his PhD in Göttingen and spent his life as a professor in Basel. Gauss's proof was geometric in nature. The French school, led by Cauchy, developed the theory of complex analysis in the 19th century and this can be used to give the "simplest" proofs of the fundamental theorem of algebra (Liouville and Rouché gave proofs; Rouché's proof in 1864 has many applications nowadays in engineering, especially in stability theory).

Purely algebraic proofs of the Fundamental Theorem of Algebra were found in the 20th century, for example Emil Artin found a proof using finite group theory, but are more difficult than the ones based on complex analysis.

Example. Let $f(x) = x^n - 1$, where n is a positive integer. Let $z_j = \cos\frac{2\pi j}{n} + i\sin\frac{2\pi j}{n}$ where $i = \sqrt{-1}$ and $j = 0, 1, 2, \cdots, n-1$.

By De Moivre's formula,

$$z_j^n = \cos\frac{2\pi jn}{n} + i\sin\frac{2\pi jn}{n}$$

$$= \cos 2\pi j + i\sin 2\pi j$$

$$= 1 + i\,0 = 1.$$

Suppose that for $j_1 \leq j_2$, $\cos\frac{2\pi j_1}{n} + i\sin\frac{2\pi j_1}{n} =$

$\cos\frac{2\pi j_2}{n} + i\sin\frac{2\pi j_2}{n}$ if and only if

$\cos\frac{2\pi j_1}{n} = \cos\frac{2\pi j_2}{n}$ and $\sin\frac{2\pi j_1}{n} = \sin\frac{2\pi j_2}{n}$.

But $\cos\theta_1 = \cos\theta_2$ and $\sin\theta_1 = \sin\theta_2$ if and only if $\theta_1 - \theta_2 = 2l\pi$ for some integer l

So $(j_1 - j_2)/n$ must be an integer, and for $0 \leq j_1 \leq j_2 \leq n-1$, this implies that $j_1 = j_2$.

$\therefore$ Hence $z_0, z_1, \cdots, z_{n-1}$ are all distinct and thus the equation $x^n - 1 = 0$ has n distinct roots in the field of complex numbers. Hence

$$x^n - 1 = (x - z_0)(x - z_1) \cdots (x - z_{n-1})$$
$$= \prod_{j=0}^{n-1} \left(x - \left(\cos \frac{2\pi j}{n} + i \sin \frac{2\pi j}{n}\right)\right).$$

<u>Examples</u>: $x^2 - 1 = (x-1)(x+1)$

$$x^3 - 1 = (x-1)\left(x - \left(\cos\frac{2\pi}{3} + i \sin\frac{2\pi}{3}\right)\right)\left(x - \left(\cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}\right)\right)$$
$$= (x-1)\left(x - \left(\frac{-1+i\sqrt{3}}{2}\right)\right)\left(x - \left(\frac{-1-i\sqrt{3}}{2}\right)\right)$$
$$x^4 - 1 = (x-1)(x-i)(x+1)(x+i).$$

If $z = a + bi$ where a, b are real numbers and $i = \sqrt{-1}$, we write $\bar{z} = a - bi$. Then $\bar{z}$ is called the complex conjugate of z. We also write $|z| = \sqrt{a^2 + b^2}$ (positive square root). $|z|$ is called the <u>absolute value</u> or <u>modulus</u> of z. Note that $z\bar{z} = |z|^2$.

<u>Simple exercise</u>: If z and w are complex numbers, then $\overline{zw} = \bar{z}\,\bar{w}$ and $|zw| = |z||w|$. Also $\overline{z+w} = \bar{z} + \bar{w}$.

If $f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$ is a polynomial with real coefficients $a_0, \cdots, a_n$ and $a_0 \neq 0$ and $n \geq 1$, then since every real number is a complex number also, we can write

$$f(x) = a_0 (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

for some complex numbers $\alpha_1, \cdots, \alpha_n$.

Since $f(\alpha_j) = 0$,

$$a_0 \alpha_j^n + a_1 \alpha_j^{n-1} + \cdots + a_n = 0$$

and taking complex conjugates and noting that $\overline{a}_r = a_r$ for each a_r since a_r is real and that $\overline{a_r \alpha_j^{n-r}} = \overline{a}_r \overline{\alpha}_j^{n-r} = \overline{a}_r (\overline{\alpha}_j)^{n-r}$ and that $\overline{z + w} = \overline{z} + \overline{w}$ for complex numbers z, w, we obtain

$$a_0 \overline{\alpha}_j^n + a_1 \overline{\alpha}_j^{n-1} + \cdots + a_n = 0$$

and $f(\overline{\alpha}_j) = 0$. So $x - \overline{\alpha}_j$ is a factor of $f(x)$. If $\alpha_j \neq \overline{\alpha}_j$, then $(x - \alpha_j)(x - \overline{\alpha}_j)$ is a factor of $f(x)$ and $(x - \alpha_j)(x - \overline{\alpha}_j) = x^2 - 2px + q$ if

$\alpha_j = p + iq$, where p and q are real numbers.

It follows that $f(x)$ can be factored, using real numbers, into a product of real polynomials of degree one or two.

If $f(x) = 0$ has all its roots real, then $f(x)$ is a product

$$a_0(x-\alpha_1)\cdots(x-\alpha_n)$$

with all α_j real.

If $f(\gamma) = 0$ for some non-real number γ, then one gets a corresponding factor

$$(x-\gamma)(x-\bar{\gamma}) = x^2 - 2cx + c^2 + d^2,$$ where

$\gamma = c + id$, c, d real and $i = \sqrt{-1}$.

<u>Example:</u>

$$x^3 + 1 = (x+1)(x^2 - x + 1)$$

$$\begin{aligned} x^4 + 4 &= (x^2+2)^2 - 4x^2 \\ &= (x^2+2)^2 - (2x)^2 \\ &= (x^2 - 2x + 2)(x^2 + 2x + 2) \end{aligned}$$

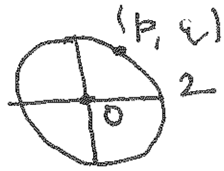
and $x^2 - x + 1$, $x^2 - 2x + 2$, $x^2 + 2x + 2$ have no real roots.

Suppose $f(x)$ is a polynomial in x of degree n, with complex coefficients. Then we know that $f(x) = 0$ has at most n distinct roots. We now consider polynomials in more than one indeterminate.

For example

$$f(x,y) = x^2 + y^2 - 4$$

is a polynomial in two indeterminates x and y and if

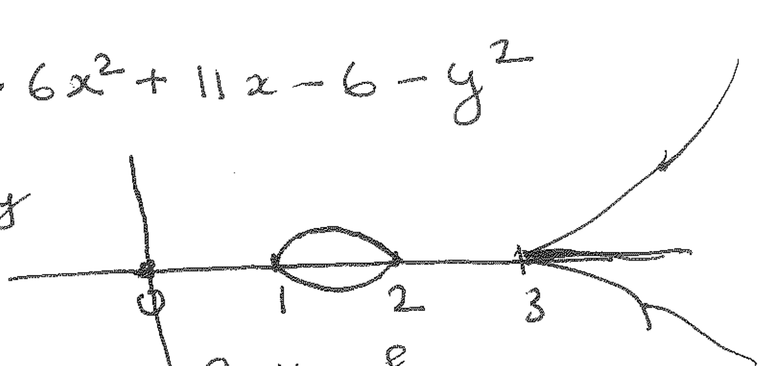


(p,q) is any point on the circle centre $(0,0)$ and radius 2, then $p^2+q^2=4$ and $f(p,q)=0$, so there are infinitely many roots (p,q) of $f(x,y)=0$ in this case.

Another example:

$$f(x,y) = x^3 - 6x^2 + 11x - 6 - y^2$$

has infinitely many roots $(x,y) = (p,q)$ with p, q real.



Graph of
$y^2 = (x-1)(x-2)(x-3)$

So there is no simple analogue of the result that a polynomial $f(x)$ (in one indeterminate) has at most n distinct roots, where $n \geq 1$ is the degree of $f(x)$. However there is a useful extension to polynomials in several indeterminates, which can be applied in some IMO type problems.

To understand the analogy, if $f(x)$ is a polynomial in the indeterminate x of degree $n \geq 1$ and A is a set of $n+1$ distinct numbers. Then we know that there is at least one element $a \in A$ for which $f(a) \neq 0$.

If $A_1, A_2, \cdots, A_k$ are sets, the Cartesian product $A_1 \times A_2 \times \cdots \times A_k$ is the set of all k-tuples

$$(a_1, a_2, \cdots, a_k).$$

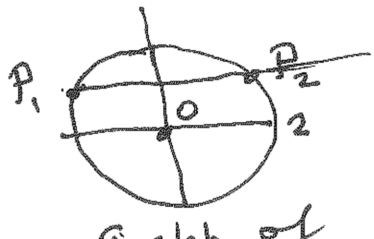
If A_j has m_j elements for $j = 1, 2, \cdots, k$, then $A_1 \times A_2 \times \cdots \times A_k$ has $m_1 m_2 \cdots m_k$ elements.

Suppose we again consider the polynomial

$$f(x, y) = x^2 + y^2 - 4$$

This has degree 2 and the term x^2 has degree 2. Think of x^2 as x^2y^0 and choose sets A_1, A_2 of numbers such that A_1 has more than 2 elements and A_2 has more than 0 elements. Say, for example, that $A_1 = \{b_1, b_2, b_3\}$ and $A_2 = \{c_1\}$. Then $A_1 \times A_2 = \{(b_1,c_1),(b_2,c_1),(b_3,c_1)\}$.

If $f(b_1,c_1) = f(b_2,c_1) = 0$,



graph of $x^2+y^2-4=0$

and $P_1(b_1,c_1)$ and $P_2(b_2,c_1)$ are the corresponding points on the circle $x^2+y^2-4=0$, then the line P_1P_2 must be parallel to the x-axis and there is no other point on this line and also on the circle. So $f(b_3,c_1) \neq 0$. The key point here is that $f(x,y)$ has degree 2, x^2y^0 is a term occurring in $f(x,y)$ of degree 2 and A_1, A_2 are two sets with A_1 having more than 2 elements and A_2 having more than 0 elements, and the conclusion is that there is at least one element $(u,v) \in A_1 \times A_2$ such that $f(u,v) \neq 0$.

Suppose $x_1, x_2, \cdots, x_k$ are distinct commuting indeterminates (or symbols). A polynomial $f(x_1, x_2, \cdots, x_k)$ is a finite sum of expressions of the form

$$a\, x_1^{l_1} x_2^{l_2} \cdots x_k^{l_k}$$

where a is a number and $l_1, l_2, \cdots, l_k$ are nonnegative integers.

<u>Example</u> $f(x_1, x_2, x_3) = 4x_1^3 x_2^2 x_3 - 7x_1 x_2^9 x_3^2 + 14 x_3^{10} - 2x_1^5 x_2^7$.

One can add, subtract and multiply such polynomials. The degree of $f(x_1, x_2, \cdots, x_k)$ is the maximum of the sums

$$l_1 + l_2 + \cdots + l_k$$

where a term

$$a\, x_1^{l_1} x_2^{l_2} \cdots x_k^{l_k}$$

occurs in $f(x_1, x_2, \cdots, x_n)$ with $a \neq 0$.

In the Example above, the sums to be looked at are $3+2+1$, $1+9+2$, 10 and $5+7$ and the maximum is 12. So $f(x_1, x_2, x_3)$ has degree 12 (In this case, two terms $-7x_1 x_2^9 x_3^2$ and $-2x_1^5 x_2^7$ both have this maximum sum 12).

One of the most famous theorems in recent times is the following:

Combinatorial Nullstellensatz of Noga Alon. (1999)

Let $f(x_1, \cdots, x_k)$ be a polynomial in $x_1, x_2, \cdots, x_k$ of degree $d \geq 1$ and let $a x_1^{l_1} x_2^{l_2} \cdots x_k^{l_k}$ be a term with $a \neq 0$ occurring in $f(x_1, \cdots, x_k)$ and having $l_1 + l_2 + \cdots + l_k = d$.

Let $A_1, A_2, \cdots, A_k$ be sets of numbers with A_j having more than l_j elements, for $j = 1, 2, \cdots, k$.

Then there exists $a_1 \in A_1$, $a_2 \in A_2$, $\cdots$, $a_k \in A_k$ with $f(a_1, a_2, \cdots, a_k) \neq 0$.

Before proving the result, we use it to solve a 2007 IMO problem.

Let n be a positive integer and

$$S = \{(x, y, z) \mid x, y, z \in \{0, 1, \cdots, n\},\ (x, y, z) \neq (0,0,0)\}.$$

is a set of $(n+1)^3 - 1$ points in 3-dimensional space. Determine the smallest number of planes whose union contains S but does not contain $(0,0,0)$.

<u>Solution:</u> The planes $x+y+z=k$ where $k = 1, 2, \cdots, 3n$, clearly have the property and their union contains all the points in S and does not contain $(0,0,0)$. So $3n$ is an upper bound for the number required.

<u>Claim</u>. We cannot use fewer than $3n$ planes.

Suppose for the sake of contradiction we can find a set of some $k < 3n$ of planes with the desired property. Suppose the equations of these planes are

$$a_j x + b_j y + c_j z - d_j = 0$$

for $j = 1, 2, \cdots, k$. Note all $d_j \neq 0$ since $(0,0,0)$ is not in any of the planes.

Let $F = (a_1 x + b_1 y + c_1 z - d_1)(a_2 x + b_2 y + c_2 z - d_2) \cdots (a_k x + b_k y + c_k z - d_k)$

and let

$$G = (x-1)(y-1)(z-1)(x-2)(y-2)(z-2) \cdots (x-n)(y-n)(z-n)$$

and let

$H = F - \alpha G$, where α is chosen so that $H(0,0,0) = 0$. [So $\alpha = \dfrac{d_1 d_2 \cdots d_k}{(-1)^{n-k}(n!)^3}$].

H has degree $3n$ and the term $x^n y^n z^n$ has coefficient $1 \neq 0$.

Let $A_1 = A_2 = A_3 = \{0, 1, 2, \cdots, n\}$.

Notice that $H(a_1, a_2, a_3) = 0$ for all $x = a_1 \in A_1$, $y = a_2 \in A_2$, $z = a_3 \in A_3$.

But each of A_1, A_2, A_3 have $n+1$ elements and $n+1 > n$ and n is the power of x, y and z, respectively, occurring in the term $x^n y^n z^n$ of highest degree.

This contradicts the Combinatorial Nullstellensatz. So $3n$ is the required number.

<u>Another example</u>. Let n and k be positive integers with $k \leq n/2$ and A a set of k integers j with $0 \leq j \leq \frac{n}{2}$. Let B be the set of integers $a_1 + a_2$, where $a_1, a_2 \in A$ with $a_1 \neq a_2$. Prove that B has at least $2k-3$ (distinct) elements.

<u>Solution</u>. Suppose B has m elements, $c_1, c_2, \cdots, c_m$, say, and form the polynomial

$$F = F(x,y) = (x-y)(x+y-c_1)(x+y-c_2)\cdots(x+y-c_m).$$

Then $F(x,y)$ has degree $m+1$.

We will show that the coefficient of the term $x^{k-1} y^{m+1-(k-1)}$ in F is nonzero, if $m \leq 2k-4$.

To get the coefficient of $x^{k-1} y^{m+1-(k-1)}$ in $F(x,y)$, observe that since this term has maximum degree among terms in $F(x,y)$, it can only arise in the product $(x-y)(x+y)^m$.

To get x^{k-1} in this product, one can choose one x from the first factor and x^{k-2} from the second factor. By the binomial theorem this can be done in $\binom{m}{k-2}$ ways. On the other hand, to get x^{k-1} in the product $(x-y)(x+y)^m$, one can choose x^{k-1} all from the second factor $(x+y)^m$ and the factor $x^{k-1} y^{m+1-(k-1)}$ then arises with coefficient $-\binom{m}{k-1}$, (the minus arises since $-y$ must be chosen in the factor $(x-y)$).

It follows that the coefficient of $x^{k-1} y^{m+1-(k-1)}$ in the polynomial

$F(x,y)$ is $\binom{m}{k-2} - \binom{m}{k-1}$. Now

$$\binom{m}{k-1} = \frac{m(m-1)\cdots(m-(k-1)+2)(m-(k-1)+1)}{(k-1)!}$$

$$= \frac{m(m-1)\cdots(m-k+3)}{(k-2)!} \cdot \frac{(m-k+2)}{k-1}$$

$$= \binom{m}{k-2} \frac{m-k+2}{k-1}.$$

Hence

$$\binom{m}{k-2} - \binom{m}{k-1} = \binom{m}{k-2}\left[1 - \frac{m-k+2}{k-1}\right]$$

and $m-k+2 \neq k-1$ if $m \neq 2k-3$.

In particular $\binom{m}{k-2} - \binom{m}{k-1} \neq 0$ if

$m \leq 2k-4$. . . (1)

Let $A_1 = A_2 = A$. Note that

$F(a_1, a_2) = 0$ for all $(a_1, a_2) \in A_1 \times A_2$. (2)

[The factor $x-y$ in $F(x,y)$ ensures this holds when $a_1 = a_2$, while if $a_1 \neq a_2$, $a_1 + a_2 = c_j$ for some j and $x+y-c_j$ is a factor of $F(x,y)$].

Now the number of elements k in A_1 is greater than $k-1$ and the number of elements k in A_2 is greater than $m+1-(k-1)$ if $m \leq 2k-4$ (even for $m \leq 2k-3$, but we need it for

$m \leq 2k-4$, in order to apply (1) above.
It now follows from (1) and this that $F(p,q) \neq 0$ for some $(p,q) \in A_1 \times A_2$, contradicting (2), if $m \leq 2k-4$. Hence $m \geq 2k-3$, as required.

Proof of the Combinatorial Nullstellensatz:

If $d=1$, then $f(x_1, \dots, x_k) = a_1x_1 + a_2x_2 + \dots + a_kx_k + b$ for some numbers $a_1, \dots, a_k$ (not all zero) and some number b. Suppose that $a_j \neq 0$.
Now A_j has at least two elements, $\alpha, \beta, \alpha \neq \beta$, say. Choose $y_t \in A_t$ for all $t \neq j$.
Then
$$P = a_1y_1 + \dots + a_{j-1}y_{j-1} + a_j\alpha + a_{j+1}y_{j+1} + \dots + a_ny_n + b$$
and
$$Q = a_1y_1 + \dots + a_{j-1}y_{j-1} + a_j\beta + a_{j+1}y_{j+1} + \dots + a_ny_n + b$$
cannot both be zero since $P-Q = a_j(\alpha-\beta)$ is not zero, as $a_j \neq 0$, $\alpha-\beta \neq 0$.
So at least one of P, Q is not zero and the conclusion of the theorem holds in this case.
This is the first step of a proof of the theorem by induction on d.

Suppose the theorem holds for all functions satisfying the hypotheses and having degree $< d =$ degree of $f(x_1, \cdots, x_k)$

For each term $b x_1^{r_1} \cdots x_k^{r_k}$, with $b \neq 0, r_1 > 0$, and occurring in $f(x_1, \cdots, x_k)$

$a_1 \in A_1$, we can write

$$x_1^{r_1} = (x_1^{r_1} - a_1^{r_1}) + a_1^{r_1}$$
$$= (x_1 - a_1)(x_1^{r_1-1} + x_1^{r_1-2} a_1 + \cdots + x_1 a_1^{r_1-2} + a_1^{r_1-1})$$
$$+ a_1^{r_1},$$

and thus

$$b x_1^{r_1} x_2^{r_2} \cdots x_k^{r_k} = (x_1 - a_1) Q_1 + R_1, \quad \cdots \text{①}$$

where $Q_1 = b(x_1^{r_1-1} + x_1^{r_1-2} a_1 + \cdots + x_1 a_1^{r_1-2} + a_1^{r_1-1}) \cdot x_2^{r_2} \cdots x_k^{r_k}$

and $R_1 = a_1^{r_1} x_2^{r_2} \cdots x_k^{r_k}$.

We can write

$$f(x_1, \cdots, x_k) = P + N,$$

where the terms in P all have x_1 occurring while x_1 does not occur in N.

Performing the above factorization on each term of P and putting all the equations of type ① together, we find $P = (x_1 - a_1) Q + R$, where $x_1^{l_1-1} x_2^{l_2} \cdots x_k^{l_k}$ occurs in the term $b x_1^{l_1-1} x_2^{l_2} \cdots x_k^{l_k}$ occurs in Q and x_1 does not occur in R.

Note that then

$$f(x_1, \cdots, x_k) = (x_1 - a_1)Q + T, \text{ where}$$

Q has degree $d-1$ and x_1 does not occur in T.

Suppose for the sake of contradiction that the theorem is not true for $f(x_1, \cdots, x_k)$ and corresponding sets $A_1, \cdots, A_k$.

So $f(u_1, u_2, \cdots, u_k) = 0$ for all $(u_1, u_2, \cdots, u_k) \in A_1 \times A_2 \times \cdots \times A_k$. ②

Since Q has degree $d-1$ and contains the element $b x_1^{l_1 - 1} x_2^{l_2} \cdots x_k^{l_k}$ of degree $d-1$ and Q satisfies the conclusions of the theorem, there must exist $(v_1, v_2, \cdots, v_k) \in A_1' \times \cdots \times A_k$ such that

$$Q(v_1, v_2, \cdots v_k) \neq 0 \quad \cdots ③$$

where here $A_1' = A_1 \setminus \{a_1\}$.

Since $f(a_1, v_2, \cdots, v_k) = 0$, it follows that $T(v_2, \cdots, v_k) = 0$, as T <u>does not involve</u> x_1. Then

Let $w_1 \in A_1 \setminus \{a_1\}$. Then $f(w_1, v_2, \cdots, v_k) = 0$ implies that $(w_1 - a_1)Q(w_1, v_2, \ldots, v_k) = 0$.

But we can take $w_1 = v_1$ and then $w_1 - a_1 \neq 0$, so

$$Q(v_1, v_2, \cdots, v_k) = 0$$

and this contradicts ③.

This contradiction arose from assuming that $f(x_1, \cdots, x_k)$ is a counterexample to the theorem. Hence no counterexample to the theorem exists and the result is proved.

[This proof is due to Michalek (Polish Acad. of Sciences, Warsaw) and is a little simpler than the original proof of Alon].

Remark. A field is a set with at least two elements on which there are defined operations called addition and multiplication satisfying the usual rules of associativity, commutativity and distributivity of "ordinary" numbers and for which every nonzero element α has an inverse element β in the set with $\alpha\beta = 1$. The rational numbers, real numbers and complex number sets are examples of fields, but not the set of integers since, for example, $1/2$ is not an integer. For p a prime number, $\mathbb{Z}_p = \{0, 1, 2, \cdots, p-1\}$ under the operations of addition and multiplication mod p, forms a field and the last theorem applies to polynomials with coefficients in $\mathbb{Z}_p$.

Exercises.

1. Let θ be a real number and $z = \cos\theta + i\sin\theta$, where $i = \sqrt{-1}$. Prove that $z + \frac{1}{z} = 2\cos\theta$ and $z - \frac{1}{z} = 2i\sin\theta$. By expanding $\left(z + \frac{1}{z}\right)^n$ and using De Moivre's Theorem, prove that if $n = 2k$ is an even positive integer, then

$$2^{n-1}\cos^n\theta = \cos n\theta + \binom{n}{1}\cos(n-2)\theta + \binom{n}{2}\cos(n-4)\theta + \cdots + \binom{n}{k-1}\cos 2\theta + \frac{1}{2}\binom{n}{k}$$

[For example, $8\cos^4\theta = \cos 4\theta + 4\cos 2\theta + 3$]. Find the corresponding formula when $n = 2k+1$ for some positive integer k.

2. Prove that $\cos\frac{\pi}{7} - \cos\frac{2\pi}{7} + \cos\frac{3\pi}{7} = \frac{1}{2}$.

3. A polynomial $f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n$ with integer coefficients has the property that $f(z)$ is divisible by 2017 for all integers z. Prove that $n!\,a_0$ is also divisible by 2017.

4. Let $n = p^2$, where p is a prime number and let $a_1 = 1 < a_2 < a_3 < \dots < a_k = p^2 - 1$ be all the positive integers l with $1 \le l < p^2$ which are not divisible by p. Calculate the number of integers r for which $a_1 + a_2 + \dots + a_r$ is divisible by p^2.