11

General homogeneous equations: Birch's theorem

We now pass to homogeneous equations in general, that is, equations which are not necessarily of the additive type considered so far. Let $f(x_1, \ldots, x_n)$ be a homogeneous polynomial, which we call a *form*, of degree k with integral coefficients. We are interested in the solubility of

$$f(x_1, \ldots, x_n) = 0$$

in integers $x_1, \ldots, x_n$ (not all 0). Owing to the homogeneity, we can allow the coefficients and variables to be rational instead of integral without changing the question. An obvious necessary condition is that the equation must be soluble in real numbers, not all 0.

When $k = 2$, so that f is a quadratic form, the general form can be expressed as an additive form by the process of 'completing the square'. It is known from the classical theory of quadratic forms that the the congruence conditions which are obviously necessary for solubility, namely the conditions that $f \equiv 0 \pmod{p^\nu}$ shall be soluble for every prime power p^ν with not all the variables divisible by p, together with the condition that the form f shall be indefinite, are also sufficient. The congruence conditions are significant only for a finite set of primes p, the set depending on the coefficients, and it is necessary that the congruences shall have a solution with $x_1, \ldots, x_n$ not all divisible by p; here also ν is determined by the coefficients. These congruence conditions are always satisfied if $n \geq 5$, accordingly we have the well known theorem of Meyer (1883) that an indefinite quadratic form in five or more variables always represents zero non-trivially.

For $k > 2$, the general form is of far greater generality than the additive form. For instance, if $k = 3$, there are $\frac{1}{6}n(n+1)(n+2)$ independent coefficients in the general form, and since a linear transformation on n

variables has only n^2 coefficients, it is plain that little simplification is possible.

An important question in connection with general forms is that of degeneration. A form in n variables is said to *degenerate* if there is a non-singular linear transformation from $x_1, \ldots, x_n$ to $y_1, \ldots, y_n$ such that the transformed form is one in $y_1, \ldots, y_{n-1}$ only; that is, the coefficients of all terms containing y_n vanish. Degeneration is an absolute property, in the sense that if a form does not degenerate by substitutions with coefficients in a particular field (e.g. the rational field), this will remain true if the field is extended. For in the above notation, we must have $\partial f/\partial y_n = 0$ identically, and if C_j is the coefficient of y_n in x_j, this is equivalent to

$$C_1 \frac{\partial f}{\partial x_1} + \cdots + C_n \frac{\partial f}{\partial x_n} = 0$$

identically. This identity represents a finite number of linear relations in the coefficients $C_1, \ldots, C_n$, and if these can be satisfied at all, they can be satisfied in the original field.

However, from the point of view of the present problem – that of representing zero – we can always suppose f non-degenerate; for if f degenerates as above, there is a solution with $x_1, \ldots, x_n$ not all 0 corresponding to the solution $y_1 = \cdots = y_{n-1} = 0$, $y_n = 1$.

The first substantial progress towards solving general homogeneous equations was made by R. Brauer [9]. He showed that, for equations with the coefficients and variables in any field, the solubility of a homogeneous equation of degree k, or of a system of homogeneous equations of degree $\leq k$, can be deduced from the solubility of every additive equation of degree $\leq k$. But the number of variables in the original equation has to be taken to be enormously large in order to get a reasonable number of variables in the final equations. In itself, the theorem cannot be applied with success in the rational field, because among the additive equations there will be some of even degree, and these will certainly not be soluble if the coefficients are all of the same sign. Brauer's theorem applies, however, in the p-adic number field, and establishes the existence of a function $n_1(k, h)$ such that any system of h homogeneous equations of degrees $\leq k$ in n variables, with p-adic coefficients, is soluble in p-adic numbers if $n \geq n_1(k, h)$.

The simplest problem in this field is that of a single cubic equation. Professor Lewis [56] was the first to prove that there exists an absolute constant n_0 such that any cubic equation $f = 0$ in n variables, with rational coefficients, is soluble in rational numbers if $n \geq n_0$. He deduced this from Brauer's result by supplementing the latter by arguments based on algebraic number theory.

Shortly afterwards, Birch [5] proved a more general theorem, namely that any system of homogeneous equations, each of odd degree, is soluble provided n exceeds a certain function of the degrees. This theorem forms the subject of the present chapter.

Before proving Birch's theorem in all its generality, I propose to explain the method in relation to the simplest case: that of a single cubic equation. It will be found that we need only to solve certain systems of linear equations in order to deduce the solubility of the general cubic equation from that of additive cubic equations. The solubility of the latter is assured by Theorem 8.1, provided the number of variables is at least $k^2(2k-1)+1 = 46$. (Actually 8 variables would suffice, but this needs special arguments.) As with Brauer's method, of which Birch's is an ingenious modification, there is a considerable wastage of variables in getting from the general form to the additive form.

Let $f(x_1, \ldots, x_n)$ be a cubic form. We say that f represents $g(y_1, \ldots, y_m)$, where $m \leq n$, if there exist n linear forms in $y_1, \ldots, y_m$, with rank m such that when $x_1, \ldots, x_n$ are replaced by these linear forms, we get

$$f(x_1, \ldots, x_n) = g(y_1, \ldots, y_m)$$

identically in $y_1, \ldots, y_m$. The essential idea of the proof is to show that f represents a form of the type

$$a_0 t_0^3 + g_1(t_1, \ldots, t_m). \tag{11.1}$$

provided n exceeds a certain number depending only on m.

Write

$$f(\mathbf{x}) = f(x_1, \ldots, x_n) = \sum_i \sum_j \sum_k c_{ijk} x_i x_j x_k,$$

where the sums go from 1 to n and where c_{ijk} is a symmetrical function of the three subscripts. Define the trilinear function $T(\mathbf{x} \,|\, \mathbf{y} \,|\, \mathbf{z})$ of three points $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$, by

$$T(\mathbf{x} \,|\, \mathbf{y} \,|\, \mathbf{z}) = \sum_i \sum_j \sum_k c_{ijk} x_i y_j z_k.$$

We choose any m linearly independent points $\mathbf{y}^{(1)}, \ldots, \mathbf{y}^{(m)}$, with integral (or rational) coordinates, and consider the equations

$$T(\mathbf{y} \,|\, \mathbf{y}^{(p)} \,|\, \mathbf{y}^{(q)}) = 0, \quad 1 \leq p \leq q \leq m$$

in an unknown point $\mathbf{y}$. These are $\frac{1}{2}m(m+1)$ linear equations in the n coordinates of $\mathbf{y}$, so if $n > \frac{1}{2}m(m+1)$ there is a point $\mathbf{y}$ other than the origin which satisfies them. Calling such a point $\mathbf{y}^{(0)}$, we have

$$T(\mathbf{y}^{(0)} \,|\, \mathbf{y}^{(p)} \,|\, \mathbf{y}^{(q)}) = 0$$

for $1 \le p \le q \le m$.

If the points $\mathbf{y}^{(0)}$, $\mathbf{y}^{(1)}$, ..., $\mathbf{y}^{(m)}$ were linearly dependent, then (since the last m are linearly independent) we should have

$$\mathbf{y}^{(0)} = c_1\mathbf{y}^{(1)} + \cdots + c_m\mathbf{y}^{(m)}$$

with rational numbers $c_1, \ldots, c_m$. But then

$$T(\mathbf{y}^{(0)} \,|\, \mathbf{y}^{(0)} \,|\, \mathbf{y}^{(0)}) = \sum_{p=1}^{m}\sum_{q=1}^{m} c_p c_q T(\mathbf{y}^{(0)} \,|\, \mathbf{y}^{(p)} \,|\, \mathbf{y}^{(q)}) = 0,$$

whence $f(\mathbf{y}^{(0)}) = 0$, giving the desired solution.

So we can suppose that the $m+1$ points are linearly independent. The transformation

$$x_j = t_0 y_j^{(0)} + t_1 y_j^{(1)} + \cdots + t_m y_j^{(m)}, \quad (1 \le j \le n)$$

has rank $m+1$, and expresses f as a form in $t_0, t_1, \ldots, t_m$. The coefficient of $t_0 t_p t_q$ in this form is $T(\mathbf{y}^{(0)} \,|\, \mathbf{y}^{(p)} \,|\, \mathbf{y}^{(q)})$, and so is 0 for $1 \le p \le q \le m$. Hence the new form is of the shape

$$a_0 t_0^3 + t_0^2(b_1 t_1 + \cdots + b_m t_m) + g_1(t_1, \ldots, t_m),$$

there being no terms of degree 1 in t_0. If $b_1, \ldots, b_m$ are all 0, we have a form of the desired type (11.1). If not, say $b_m \ne 0$, we put

$$t_m = -\frac{1}{b_m}(b_1 t_1 + \cdots + b_{m-1} t_{m-1})$$

and obtain a form of the type (11.1) but with $m-1$ instead of m. Hence f represents a form of the type (11.1) provided only that $n > \frac{1}{2}m(m+1)$. We can suppose in (11.1) that $a_0 \ne 0$, for if $a_0 = 0$ there is a solution in $x_1, \ldots, x_n$ corresponding to $t_0 = 1$, $t_1 = \cdots = t_m = 0$.

We see that we can have m as large as we please by taking n sufficiently large. Also we can repeat the process on the new form $g(t_1, \ldots, t_m)$, which can be assumed not to represent zero. It follows that there is a function $n_0(s)$ such that, if $n \ge n_0(s)$, the form f represents a form of the type

$$b_1 u_1^3 + \cdots + b_s u_s^3.$$

By Theorem 8.1, the corresponding homogeneous equation has a non-trivial solution if $s \geq s_0$ (= 46, say), and hence the original equation is soluble if $n \geq n_0(s_0)$.

We now prove Birch's general theorem:

Theorem 11.1. *Let h, m be positive integers, and let $r_1, \ldots, r_h$ be any odd positive integers. Then there exists a number*

$$\Psi(r_1, \ldots, r_h; m)$$

with the following property. Let $f_{r_1}(\mathbf{x}), \ldots, f_{r_h}(\mathbf{x})$ be forms of degrees $r_1, \ldots, r_h$ respectively in $\mathbf{x} = (x_1, \ldots, x_n)$, with rational coefficients. Then, provided $n \geq \Psi(r_1, \ldots, r_h; m)$, there is an m-dimensional rational vector space, all points in which satisfy

$$f_{r_1}(\mathbf{x}) = 0, \ldots, f_{r_h}(\mathbf{x}) = 0.$$

Note that we assert more than the existence of an infinity of solutions; this is for convenience in the inductive proof.

Lemma 11.1. *There exists a number $\Phi(r, m)$, defined for positive integers m, r with r odd, such that if $s \geq \Phi(r, m)$, any equation of the form*

$$c_1 x_1^r + \cdots + c_s x_s^r = 0, \quad (c_j \textit{ rational})$$

is satisfied by all points of some rational linear space of dimension m.

Proof. The result is a simple deduction from Theorem 8.1 or Theorem 10.1. By either of these theorems there exists $t = t(r)$ such that the equation

$$c_1 y_1^r + \cdots + c_t y_t^r = 0$$

has a non-zero integral solution. Note that since r is odd, there is no condition on the signs of the coefficients; also if any of them is 0 there is an obvious solution. Similarly for the equation

$$c_{t+1} y_{t+1}^r + \cdots + c_{2t} y_{2t}^r = 0,$$

and so on. Hence, if $s \geq mt$, the point

$$(u_1 y_1, \ldots, u_1 y_t, u_2 y_{t+1}, \ldots, u_2 y_{2t}, \ldots, u_m y_{mt}, 0, \ldots, 0)$$

formed out of these solutions, satisfies the equation for all values of $u_1, \ldots, u_m$. As these vary, the point describes an m-dimensional linear space. Hence the result, with $\Psi(r, m) = mt$. □

Proof of Theorem 11.1. Let $R = \max r_j$, so that R is an odd positive integer. The result certainly holds when $R = 1$, and we prove it by induction on R (limited to odd values). We shall first prove that if the result holds for systems of equations with $\max r_j \le R-2$, then it holds for a single equation of degree R. Once this has been proved, it will be easy to extend the result to a system of equations of degree $\le R$, and thereby complete the inductive proof.

For a form $f(x_1, \ldots, x_n)$ of degree R, we define a multilinear function of R points $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(R)}$ by

$$\begin{aligned} f(x_1, \ldots, x_n) &= \sum c_{i_1,\ldots,i_R} x_{i_1} \ldots x_{i_R}, \\ M(\mathbf{x}^{(1)} \mid \cdots \mid \mathbf{x}^{(R)}) &= \sum c_{i_1,\ldots,i_R} x_{i_1}^{(1)} \ldots x_{i_R}^{(R)}. \end{aligned}$$

We begin by selecting h linearly independent points $\mathbf{y}^{(1)}, \ldots, \mathbf{y}^{(h)}$. Let $\mathcal{Y}$ be the h-dimensional linear space generated by them. Consider the equations

$$M(\underbrace{\mathbf{y} \mid \cdots \mid \mathbf{y}}_{\rho} \mid \mathbf{y}^{(p_1)} \mid \cdots \mid \mathbf{y}^{(p_{R-\rho})}) = 0,$$

where ρ takes all odd values from 1 to $R-2$, and $p_1, \ldots, p_{R-\rho}$ take all values from 1 to h. The total number of equations is less than Rh^R. Each of them is of odd degree $\le R-2$ in $\mathbf{y}$. Hence, by the inductive hypothesis (for $m = 1$) these equations have a non-zero solution in $\mathbf{y}$ provided $n \ge n_0(R, h)$. Denote such a solution by $\mathbf{y}^{(0)}$. We now have

$$M(\underbrace{\mathbf{y}^{(0)} \mid \cdots \mid \mathbf{y}^{(0)}}_{\rho} \mid \underbrace{\mathbf{y} \mid \cdots \mid \mathbf{y}}_{R-\rho}) = 0$$

for all y in $\mathcal{Y}$ and all odd $\rho \le R-2$.

An arbitrary point $\mathbf{y}$ in $\mathcal{Y}$ is of the form

$$u_1\mathbf{y}^{(1)} + \cdots + u_h\mathbf{y}^{(h)}.$$

Now consider the equations

$$M(\underbrace{\mathbf{y}^{(0)} \mid \cdots \mid \mathbf{y}^{(0)}}_{R-\sigma} \mid \underbrace{\mathbf{y} \mid \cdots \mid \mathbf{y}}_{\sigma}) = 0,$$

where σ takes all odd values from 1 to $R-2$, and $\mathbf{y}$ is any point in $\mathcal{Y}$. These are equations of odd degree $\le R-2$ in $u_1, \ldots, u_h$, and their number is $< R$. By the inductive hypothesis again, given any ℓ, these equations will be satisfied at all points of some rational linear subspace of $\mathcal{Y}$ of dimension $\ell+1$, provided $h \ge h_0(R, \ell)$. Denote this linear subspace by $\mathcal{Y}_1$. We can suppose, without loss of generality, that $\mathcal{Y}_1$ is generated by $\mathbf{y}^{(1)}, \ldots, \mathbf{y}^{(\ell+1)}$. We now have

$$M(\underbrace{\mathbf{y}^{(0)} \mid \cdots \mid \mathbf{y}^{(0)}}_{\tau} \mid \underbrace{\mathbf{y} \mid \cdots \mid \mathbf{y}}_{R-\tau}) = 0$$

for all $\tau = 1, \ldots, R-1$ and for all $\mathbf{y}$ in the $(\ell+1)$-dimensional space $\mathcal{Y}_1$. To ensure this we need only suppose that $n \geq n_0(R, h_0(R, \ell)) = n_1(R, \ell)$.

If $\mathbf{y}^{(0)}$ is in the subspace $\mathcal{Y}_1$, generated by $\mathbf{y}^{(1)}, \ldots, \mathbf{y}^{(\ell+1)}$, we can obtain an ℓ-dimensional subspace $\mathcal{Y}_2$ of $\mathcal{Y}_1$ which does not contain $\mathbf{y}^{(0)}$ by omitting one of the generating points $\mathbf{y}^{(1)}, \ldots, \mathbf{y}^{(\ell+1)}$, say the last. Now the points $\mathbf{y}^{(0)}, \mathbf{y}^{(1)}, \ldots, \mathbf{y}^{(\ell)}$ are linearly independent. The linear transformation

$$x_j = t_0 y_j^{(0)} + \cdots + t_\ell y_j^{(\ell)}, \quad (1 \leq j \leq n)$$

has rank $\ell + 1$ and gives $f(\mathbf{x}) = g(t_0, \ldots, t_\ell)$, say. The coefficient of $t_0^\tau t_{p_1} \cdots t_{p_{R-\tau}}$ in g (where each p_j goes from 1 to ℓ) is

$$M(\mathbf{y}^{(0)} \mid \cdots \mid \mathbf{y}^{(0)} \mid \mathbf{y}^{(p_1)} \mid \cdots \mid \mathbf{y}^{(p_{R-\tau})}) = 0,$$

and this holds for $\tau = 1, \ldots, R-1$ and any choice of $p_1, \ldots, p_{R-\tau}$. Hence

$$g(t_0, \ldots, t_\ell) = a_0 t_0^R + g_1(t_1, \ldots, t_\ell).$$

Hence f represents a form of the above type, for any ℓ, provided $n \geq n_1(R, \ell)$. Repetition of the argument proves that f represents a form of the type

$$\underbrace{a_0 t_0^R + b_0 u_0^R + \cdots}_{s}$$

provided $n \geq n_2(R, s)$. By Lemma 11.1, the solutions of the homogeneous equation obtained by equating the latter form to 0 include a linear space of dimension m provided $s \geq \Phi(r, m)$. Hence the solutions of the original equation include a linear space of dimension m provided $n \geq n_2(R, \Phi(R, m))$. This proves the desired result for a single equation of degree R.

Now suppose there are h equations $f_{r_1} = 0, \ldots, f_{r_h} = 0$, where each $r_j \leq R$. We prove the result by induction on h, the case $h = 1$ being what we have just proved. Given m_1 there exists a rational linear space of dimension m_1 on which $f_{r_h} = 0$, provided $n \geq \Psi(r_h; m_1)$, by the case $h = 1$ of the theorem. We can represent the points of this linear space as

$$v_1 \mathbf{x}^{(1)} + \cdots + v_{m_1} \mathbf{x}^{(m_1)}.$$

For these points, the forms $f_{r_1}, \ldots, f_{r_{h-1}}$ become forms in $v_1, \ldots, v_{m_1}$. By the case $h-1$, there is a linear space of dimension m on which they all vanish, provided $m_1 \geq \Psi(r_1, \ldots, r_{h-1}; m)$. Hence all the forms vanish on this space, and the case h of the theorem holds, with

$$\Psi(r_1, \ldots, r_h; m) = \Psi(r_h; \Psi(r_1, \ldots, r_{h-1}; m)).$$

This completes the proof. $\square$

Corollary. *Theorem 11.1 continues to hold if the forms have coefficients in an algebraic number field K and $x_1, \ldots, x_n$ have values in K, but with Ψ depending now on K.*

When we express each coefficient and each variable linearly in terms of a basis of K (say $\{1, \theta, \ldots, \theta^{\nu-1}\}$, where ν is the degree of K and θ a generating element), each equation is equivalent to ν equations of the same degree with rational coefficients and variables.

Our next aim will be to prove a more precise result concerning the number of variables which will suffice to make one homogeneous cubic equation soluble. In the course of the work we shall need some results from the geometry of numbers, and so we begin with an account of certain aspects of this subject.