Chapter 7

The Subspace Theorem

Literature:
W.M. Schmidt, Diophantine approximation, Lecture Notes in Mathematics 785, Springer Verlag 1980, Chap.IV,VI,VII

The Subspace Theorem is a higher dimensional generalization of Roth's Theorem on the approximation of algebraic numbers by rational numbers. We explain the Subspace Theorem, give some applications to simultaneous Diophantine approximation, and then an application to higher dimensional generalizations of Thue equations, the so-called *norm form equations*.

7.1 The Subspace Theorem and some applications

In the formulation of the Subspace Theorem, we need some notions from linear algebra, which we recall below. Let n be an integer $\geqslant 1$ and $r \leqslant n$. We say that linear forms $L_1 = \sum_{j=1}^n \alpha_{1j} X_j$, ..., $L_r = \sum_{j=1}^n \alpha_{nj} X_j$ with coefficients in $\mathbb{C}$ are linearly dependent if there are $c_1, \ldots, c_r \in \mathbb{C}$, not all 0, such that $c_1 L_1 + \cdots + c_r L_r \equiv 0$. Otherwise, $L_1, \ldots, L_r$ are called linearly independent. If $r = n$, then $L_1, \ldots, L_n$ are linearly independent if and only if their coefficient determinant $\det(L_1, \ldots, L_n) = \det(\alpha_{ij})_{1 \leqslant i,j \leqslant n} \neq 0$.

A linear subspace T of $\mathbb{Q}^n$ of dimension r can be described as

$$T = \left\{ \sum_{i=1}^r z_i \mathbf{a}_i : \, z_1, \ldots, z_r \in \mathbb{Q} \right\},$$

where $\mathbf{a}_1, \ldots, \mathbf{a}_r$ are linearly independent vectors from $\mathbb{Q}^n$, or alternatively as

$$T = \{\mathbf{x} \in \mathbb{Q}^n : L_1(\mathbf{x}) = 0, \ldots, L_{n-r}(\mathbf{x}) = 0\}$$

where $L_1, \ldots, L_{n-r}$ are linearly independent linear forms in $X_1, \ldots, X_n$ with coefficients from $\mathbb{Q}$.

As before, $\overline{\mathbb{Q}}$ is the field of complex numbers that are algebraic over $\mathbb{Q}$. For the norm of $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ we always take the maximum norm, i.e.,

$$\|\mathbf{x}\| := \max(|x_1|, \ldots, |x_n|).$$

Theorem 7.1. (Subspace Theorem, W.M. Schmidt, 1972). *Let $n \geqslant 2$, let*

$$L_i = \alpha_{i1}X_1 + \cdots + \alpha_{in}X_n \quad (i = 1, \ldots, n)$$

be n ***linearly independent linear forms with coefficients in*** $\overline{\mathbb{Q}}$ *and let $C > 0$, $\delta > 0$. Then the set of solutions of the inequality*

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| \leqslant C\|\mathbf{x}\|^{-\delta} \text{ in } \mathbf{x} \in \mathbb{Z}^n \tag{7.1}$$

is contained in a union $T_1 \cup \cdots \cup T_t$ of finitely many proper linear subspaces of $\mathbb{Q}^n$.

Remark. The proof of the Subspace Theorem is *ineffective*, i.e., it does not enable to determine the subspaces. There is however a quantitative version of the Subspace Theorem which gives an explicit upper bound for the *number* of subspaces. This is an important tool for deriving upper bounds for the number of solutions of various types of Diophantine equations.

We show that the Subspace Theorem implies Roth's Theorem. Recall that the height of $\xi \in \mathbb{Q}$ is $H(\xi) = \max(|x|, |y|)$, where $\xi = x/y$ with $x, y \in \mathbb{Z}$, $\gcd(x, y) = 1$.

Corollary 7.2. *Let $\alpha \in \overline{\mathbb{Q}}$ and $C > 0$, $\kappa > 2$. Then the inequality*

$$|\xi - \alpha| \leqslant C \cdot H(\xi)^{-\kappa} \text{ in } \xi \in \mathbb{Q} \tag{7.2}$$

has only finitely many solutions.

Proof. Let $\xi = x/y$ be a solution of (7.2), with $x, y \in \mathbb{Z}$, $\gcd(x, y) = 1$. Write $\kappa = 2 + \delta$ with $\delta > 0$. By multiplying (7.2) with y^2 we obtain

$$|y(x - \alpha y)| \leqslant Cy^2 \max(|x|, |y|)^{-2-\delta} \leqslant C \cdot \max(|x|, |y|)^{-\delta}.$$

Since the linear forms Y and $X - \alpha Y$ are linearly independent, this is an inequality to which the Subspace Theorem is applicable. It follows that the pairs of integers $(x, y) \in \mathbb{Z}^2$ with $\gcd(x, y) = 1$ such that $\xi = x/y$ is a solution of (7.2) lie in a union of finitely many proper, i.e., one-dimensional linear subspaces of $\mathbb{Q}^2$. But a given one-dimensional subspace of $\mathbb{Q}^2$ consists of all points of the shape $\lambda(x_0, y_0)$ with $\lambda \in \mathbb{Q}$ where $(x_0, y_0) \in \mathbb{Z}^2$, thus the rational number ξ is uniquely determined by the subspace. This proves Roth's Theorem. $\square$

The Subspace Theorem states that the set of solutions of (7.1) is contained in a finite union of proper linear subspaces of $\mathbb{Q}^n$, but one may wonder whether (7.1) has only finitely many solutions. For instance, it may be that there is a non-zero $\mathbf{x}_0 \in \mathbb{Z}^n$ with $L_1(\mathbf{x}_0) = 0$. Then for every $\lambda \in \mathbb{Z}$, the point $\lambda \mathbf{x}_0$ is a solution to (7.1), and this gives infinitely many solutions to (7.1). To avoid such a construction, let us consider

$$0 < |L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| \leqslant C \cdot \|\mathbf{x}\|^{-\delta} \text{ in } \mathbf{x} \in \mathbb{Z}^n. \tag{7.3}$$

In the case $n = 2$ the number of solutions is indeed finite.

Lemma 7.3. *Let $L_i = \alpha_{i1} X + \alpha_{i2} Y$ $(i = 1, 2)$ be two linearly independent linear forms with coefficients in $\overline{\mathbb{Q}}$ and let $C > 0, \delta > 0$. Then the inequality*

$$0 < |L_1(\mathbf{x}) L_2(\mathbf{x})| \leqslant C \|\mathbf{x}\|^{-\delta} \quad \textit{in } \mathbf{x} = (x, y) \in \mathbb{Z}^2 \tag{7.4}$$

has only finitely many solutions.

Proof. By the Subspace Theorem, the solutions of (7.4) lie in finitely many one-dimensional linear subspaces of $\mathbb{Q}^2$. So we have to prove that each of these subspaces contains only finitely many solutions. Let T be one of these subspaces. Then $T = \{\lambda \mathbf{x}_0 : \lambda \in \mathbb{Q}\}$ where we may choose $\mathbf{x}_0 = (x_0, y_0) \in \mathbb{Z}^2$ with $\gcd(x_0, y_0) = 1$. Note that $\lambda(x_0, y_0) \in \mathbb{Z}^2$ if and only if $\lambda \in \mathbb{Z}$. If $L_1(\mathbf{x}_0) L_2(\mathbf{x}_0) = 0$ then (7.4) has no solutions in T. Suppose that $L_1(\mathbf{x}_0) L_2(\mathbf{x}_0) \neq 0$. Then $\mathbf{x} = \lambda \mathbf{x}_0$ is a solution of (7.4) if and only if

$$0 < \lambda^2 |L_1(\mathbf{x}_0) L_2(\mathbf{x}_0)| \leqslant C \cdot |\lambda|^{-\delta} \|\mathbf{x}_0\|^{-\delta},$$

i.e., if $|\lambda|^{2+\delta} \leqslant C \|\mathbf{x}_0\|^{-\delta} |L_1(\mathbf{x}_0) L_2(\mathbf{x}_0)|^{-1}$. This shows that $|\lambda|$ is bounded, hence that T contains only finitely many solutions of (7.4). $\square$

However, if $n \geqslant 3$, then (7.3) may very well have infinitely many solutions. We illustrate this with an example.

Example. Let $0 < \delta < 1$ and consider the inequality

$$(7.5)\quad 0 < |(x_1 + \sqrt{2}x_2 + \sqrt{3}x_3)(x_1 - \sqrt{2}x_2 + \sqrt{3}x_3)(x_1 - \sqrt{2}x_2 - \sqrt{3}x_3)| \leqslant \|\mathbf{x}\|^{-\delta}$$

to be solved in $\mathbf{x} = (x_1, x_2, x_3) \in \mathbb{Z}^3$. Notice that the three linear forms on the left-hand side are linearly independent.

Consider the triples of integers $\mathbf{x} = (x_1, x_2, x_3) \in \mathbb{Z}^3$ with $x_3 = 0, x_1x_2 \neq 0$. For these points, $\|\mathbf{x}\| = \max(|x_1|, |x_2|, 0)$. By Dirichlet's Theorem, the inequality

$$\left|\sqrt{2} - \frac{x_1}{x_2}\right| \leqslant |x_2|^{-2}$$

has infinitely many solutions $(x_1, x_2) \in \mathbb{Z}^2$ with $x_2 \neq 0$. For these solutions, $\|\mathbf{x}\|$ has the same order of magnitude as $|x_2|$. Indeed,

$$|x_1/x_2| \leqslant |x_2|^{-2} + \sqrt{2} \leqslant 1 + \sqrt{2},$$

and so, $\|\mathbf{x}\| = \max(|x_1|, |x_2|) \leqslant (1 + \sqrt{2})|x_2|$.

So for the points under consideration,

$$\begin{aligned} 0 &< |(x_1 + \sqrt{2}x_2 + \sqrt{3}x_3)(x_1 - \sqrt{2}x_2 + \sqrt{3}x_3)(x_1 - \sqrt{2}x_2 - \sqrt{3}x_3)| \\ &= |(x_1 + \sqrt{2}x_2)(x_1 - \sqrt{2}x_2)^2| \\ &\leqslant (1 + \sqrt{2})\|\mathbf{x}\| \cdot (x_2^{-1})^2 \leqslant (1 + \sqrt{2})^3\|\mathbf{x}\|^{-1} \\ &\leqslant \|\mathbf{x}\|^{-\delta}, \end{aligned}$$

provided $\|\mathbf{x}\|$ is sufficiently large. It follows that (7.5) has infinitely many solutions $\mathbf{x}$ in the subspace $x_3 = 0$.

We state a convenient reformulation of the Subspace Theorem. Let $L_1, \ldots, L_r$ be linear forms with coefficients in $\mathbb{C}$ in the variables $X_1, \ldots, X_n$, where $r \geqslant n$. We say that $L_1, \ldots, L_r$ (or more correctly the hyperplanes $L_1 = 0, \ldots, L_r = 0$ being defined by them) are *in general position* if each n-tuple of linear forms among $L_1, \ldots, L_r$ is linearly independent.

Theorem 7.4. *Let*

$$L_i = \alpha_{i1}X_1 + \cdots + \alpha_{in}X_n \quad (i = 1, \ldots, r,\ r \geqslant n)$$

be r linear forms with coefficients in $\overline{\mathbb{Q}}$ in general position and let $C > 0$, $\delta > 0$. Then the set of solutions of the inequality

$$|L_1(\mathbf{x}) \cdots L_r(\mathbf{x})| \leqslant C \cdot \|\mathbf{x}\|^{r-n-\delta} \text{ in } \mathbf{x} \in \mathbb{Z}^n \tag{7.6}$$

is contained in a union $T_1 \cup \cdots \cup T_t$ of finitely many proper linear subspaces of $\mathbb{Q}^n$.

This is in fact equivalent to the basic Subspace Theorem 7.1. The implication Theorem 7.4 $\Rightarrow$ Theorem 7.1 is clear. The other implication Theorem 7.1 $\Rightarrow$ Theorem 7.4 is proved by means of the following lemma.

Lemma 7.5. *Let $M_1, \ldots, M_n$ be linearly independent linear forms in $X_1, \ldots, X_n$ with complex coefficients. Then there is a constant $C > 0$ such that*

$$\|\mathbf{x}\| \leqslant C \max\big(|M_1(\mathbf{x})|, \ldots, |M_n(\mathbf{x})|\big) \quad \text{for all } \mathbf{x} \in \mathbb{C}^n.$$

Proof. Since the linear forms $M_1, \ldots, M_n$ are linearly independent, they span the complex vector space of all linear forms in $X_1, \ldots, X_n$ with complex coefficients. So we can express $X_1, \ldots, X_n$ as linear combinations of $M_1, \ldots, M_n$, i.e.,

$$X_i = \sum_{j=1}^{n} \beta_{ij} M_j \text{ with } \beta_{ij} \in \mathbb{C} \ (i = 1, \ldots, n).$$

Take $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{C}^n$ and put $M := \max_{1 \leqslant i \leqslant n} |M_i(\mathbf{x})|$. Then

$$\max_{1 \leqslant i \leqslant n} |x_i| \leqslant \max_{1 \leqslant i \leqslant n} \sum_{j=1}^{n} |\beta_{ij}| \cdot |M_j(\mathbf{x})| \leqslant C \cdot M \quad \text{with } C := \max_{1 \leqslant i \leqslant n} \sum_{j=1}^{n} |\beta_{ij}|.$$

□

Proof of Theorem 7.4 from Theorem 7.1. We partition the solutions $\mathbf{x}$ of (7.6) into a finite number of subsets according to the ordering of the numbers $|L_1(\mathbf{x})|, \ldots, |L_r(\mathbf{x})|$, and show that each of these subsets lies in at most finitely many proper linear subspaces of $\mathbb{Q}^n$. Consider the solutions $\mathbf{x} \in \mathbb{Z}^n$ from one of these subsets, say for which

$$|L_1(\mathbf{x})| \leqslant \cdots \leqslant |L_r(\mathbf{x})|. \tag{7.7}$$

Let $i \in \{n+1, \dots, r\}$. Then the linear forms $L_1, \dots, L_{n-1}, L_i$ are linearly independent, so by Lemma 7.5, there is a constant C_i such that for all solutions $\mathbf{x}$ of (7.6) with (7.7),

$$\|\mathbf{x}\| \leqslant C_i \max(|L_1(\mathbf{x})|, \dots, |L_{n-1}(\mathbf{x})|, |L_i(\mathbf{x})|) = C_i |L_i(\mathbf{x})|.$$

Inserting this into (7.6) for $i = n+1, \dots, r$ we obtain that the solutions of (7.6) with (7.7) satisfy

$$\begin{aligned} |L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| &\leqslant C \|\mathbf{x}\|^{r-n-\delta} \prod_{i=n+1}^{r} |L_i(\mathbf{x})|^{-1} \\ &\leqslant C \cdot (C_{n+1} \cdots C_r) \|\mathbf{x}\|^{-\delta}, \end{aligned}$$

and thus, by Theorem 7.1, lie in at most finitely many proper linear subspaces of $\mathbb{Q}^n$. □

We present some further applications of the Subspace Theorem. Before doing this, we give a slight variation on a theorem of Dirichlet.

Lemma 7.6. *Let $\alpha_1, \dots, \alpha_n \in \mathbb{R}$ be numbers that are linearly independent over $\mathbb{Q}$. Then there is $C > 0$ such that the inequality*

(7.8) $$|\alpha_1 x_1 + \cdots + \alpha_n x_n| \leqslant C \cdot \|\mathbf{x}\|^{1-n} \text{ in } \mathbf{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n$$

has infinitely many solutions.

Proof. Without loss of generality, $|\alpha_n| = \max_{1 \leqslant i \leqslant n} |\alpha_i|$. Let $\beta_i = -\alpha_i/\alpha_n$ ($i = 1, \dots, n-1$); then $|\beta_i| \leqslant 1$ for $i = 1, \dots, n-1$. For instance from Minkowski's convex body theorem (see Chapter 2), one deduces that there are infinitely many $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n$ such that at least one of $x_1, \dots, x_{n-1}$ is non-zero, and

(7.9) $$|x_n - \beta_1 x_1 - \cdots - \beta_{n-1} x_{n-1}| \leqslant \max(|x_1|, \dots, |x_{n-1}|)^{1-n},$$

Given a solution of this inequality, it follows easily that

$$|x_n| \leqslant 1 + \sum_{i=1}^{n-1} |\beta_i| \cdot |x_i| \leqslant n \max_{1 \leqslant i \leqslant n-1} |x_i|,$$

say, hence $\|\mathbf{x}\| \leqslant n \max_{1 \leqslant i \leqslant n-1} |x_i|$. By inserting this into (7.9) and multiplying with $|\alpha_n|$ we get (7.8) with $C = |\alpha_n| \cdot n^{n-1}$. □

From the Subspace Theorem we deduce that the exponent $1-n$ in (7.8) cannot be replaced by something smaller if the coefficients α_i are all algebraic.

Theorem 7.7. *Let $\alpha_1,\dots,\alpha_n \in \overline{\mathbb{Q}}$ and $C>0, \delta>0$. Then the inequality*

$$0 < |\alpha_1 x_1 + \cdots + \alpha_n x_n| \leqslant C \cdot \|\mathbf{x}\|^{1-n-\delta} \text{ in } \mathbf{x} = (x_1,\dots,x_n) \in \mathbb{Z}^n \tag{7.10}$$

has only finitely many solutions.

Remark. For $n=2$ this implies Roth's Theorem. Indeed, let $C>0$, $\kappa>2$ and let α be an irrational algebraic number. Take a solution $\xi = x/y$ (with coprime integers x,y) of $|\alpha-\xi| \leqslant C \cdot H(\xi)^{-\kappa}$. Then multiplying with y gives

$$0 < |x-\alpha y| \leqslant C \cdot |y| \cdot \max(|x|,|y|)^{-\kappa} \leqslant C \max(|x|,|y|)^{1-\delta}$$

where $\delta = \kappa - 2$. By the above theorem, the latter inequality has only finitely many solutions $(x,y) \in \mathbb{Z}^2$. This leaves only finitely many possibilities for ξ.

Proof of Theorem 7.7. We proceed by induction on n. For $n=1$ the assertion is obvious. (Here we use our assumption $\alpha_1 x_1 \neq 0$). Let $n>1$ and suppose Theorem 7.7 is true for linear forms in fewer than n variables.

We apply the Subspace Theorem. We may assume that at least one of the coefficients $\alpha_1,\dots,\alpha_n$ is non-zero, otherwise there are no solutions. Suppose that $\alpha_1 \neq 0$. Then (7.10) implies

$$|(\alpha_1 x_1 + \cdots + \alpha_n x_n) x_2 \cdots x_n| \leqslant C\|\mathbf{x}\|^{-\delta}$$

and by the Subspace Theorem, the solutions of the latter lie in a union of finitely many proper linear subspaces $T_1,\dots,T_t$ of $\mathbb{Q}^n$. We consider only solutions with $\alpha_1 x_1 + \cdots + \alpha_n x_n \neq 0$. Therefore, without loss of generality we may assume that $\alpha_1 x_1 + \cdots + \alpha_n x_n$ is not identically 0 on any of the spaces $T_1,\dots,T_t$.

Consider the solutions of (7.6) in T_i. Choose a non-trivial linear form vanishing identically on T_i, $a_1 x_1 + \cdots + a_n x_n = 0$. Suppose for instance, that $a_n \neq 0$. Then x_n can be expressed as a linear combination of $x_1,\dots,x_{n-1}$. By substituting this into (7.10) we obtain an inequality

$$0 < |\beta_1 x_1 + \cdots + \beta_{n-1} x_{n-1}| \leqslant C\|\mathbf{x}\|^{1-n-\delta} \leqslant C\big(\max_{1\leqslant i\leqslant n-1} |x_i|\big)^{2-n-\delta}.$$

By the induction hypothesis, the latter inequality has only finitely many solutions $(x_1,\dots,x_{n-1})$. So T_i contains only finitely many solutions $\mathbf{x}$ of (7.6). Applying this to $T_1,\dots,T_t$ we obtain that (7.10) has altogether only finitely many solutions. □

Instead of approximating a given algebraic number α by rationals, we can also consider the approximation of α by algebraic numbers of degree at most d. Recall that the primitive minimal polynomial of $\xi \in \overline{\mathbb{Q}}$ is the polynomial $F := a_0X^d + a_1X^{d-1} + \cdots + a_d \in \mathbb{Z}[X]$ such that $F(\xi) = 0$, F is irreducible, and $a_0 > 0$, $\gcd(a_0, \ldots, a_d) = 1$. Then the height of ξ is $H(\xi) := \max(|a_0|, \ldots, |a_d|)$.

We consider

$$|\xi - \alpha| \leqslant C \cdot H(\xi)^{-\kappa} \quad \text{in } \xi \in \overline{\mathbb{Q}} \text{ with } \deg \xi \leqslant d. \tag{7.11}$$

Theorem 7.8. *For every $C > 0$, $\kappa > d+1$, inequality (7.11) has only finitely many solutions.*

Proof. Write $\kappa = d + 1 + \delta$ with $\delta > 0$. Let ξ be a solution of (7.11). Let $F = x_0 + x_1X + \cdots + x_dX^d$ be the primitive minimal polynomial of ξ. Then $\mathbf{x} := (x_0, \ldots, x_d) \in \mathbb{Z}^{d+1}$ and $H(\xi) = \|\mathbf{x}\|$. We want to show that there are only finitely many possibilities for F, and to this end, we want to estimate from above $|F(\alpha)| = |\sum_{i=0}^{d} x_i\alpha^i|$ and apply Theorem 7.7.

Since $F(\xi) = 0$ we have

$$|F(\alpha)| = \Big| \int_0^1 F'(\xi + t(\alpha - \xi)) \cdot (\alpha - \xi)dt \Big| \leqslant |\alpha - \xi| \cdot \max_{0 \leqslant t \leqslant 1} |F'(\xi + t(\alpha - \xi))|.$$

Using $|\xi + t(\alpha - \xi)| \leqslant |\alpha| + |\xi| \leqslant |\alpha| + C$ for $0 \leqslant t \leqslant 1$, we obtain

$$|F'(\xi + t(\alpha - \xi))| \leqslant \sum_{i=1}^{d} |x_i| \cdot i(|\alpha| + C)^{i-1} \leqslant C'\|\mathbf{x}\|,$$

say. Hence $|F(\alpha)| \leqslant |\xi - \alpha| \cdot C'\|\mathbf{x}\|$. There are only finitely many ξ that are conjugate to α. For the remaining solutions ξ of (7.11) we have $F(\alpha) \neq 0$, and so

$$0 < |\sum_{i=0}^{d} x_i\alpha^i| = |F(\alpha)| \leqslant C'\|\mathbf{x}\| \cdot |\xi - \alpha| \leqslant C' \cdot C\|\mathbf{x}\|^{-d-\delta}.$$

By Theorem 7.8 with $n = d + 1$, this has at most finitely many solutions $\mathbf{x} \in \mathbb{Z}^{d+1}$. These give rise to at most finitely many possibilities for F, hence to at most finitely many possibilities for ξ. $\square$

7.2 Norm form equations

Let α be an algebraic number of degree d, and let $\alpha^{(1)}, \ldots, \alpha^{(d)}$ be its conjugates. Consider the binary form

$$F(X, Y) = \prod_{i=1}^{d} (X - \alpha^{(i)} Y).$$

In fact, $F(X, 1)$ is the minimal polynomial of α, hence it is an irreducible polynomial in $\mathbb{Q}[X]$. So $F(X, Y)$ is irreducible in $\mathbb{Q}[X, Y]$. Let $K = \mathbb{Q}(\alpha)$. Then σ_i, with $\sigma_i(\alpha) := \alpha^{(i)}$ $(i = 1, \ldots, d)$ are the embeddings of K in $\mathbb{C}$. Extending the norm $N_{K/\mathbb{Q}}(\cdot) = \prod_{i=1}^{d} \sigma_i(\cdot)$ on K to polynomials with coefficients in K, we get

$$F(X, Y) = \prod_{i=1}^{d} (X - \sigma_i(\alpha) Y) = N_{K/\mathbb{Q}}(X - \alpha Y).$$

That is, F is a *norm form* in two variables. The equation

$$F(x, y) = N_{K/\mathbb{Q}}(x - \alpha y) = c \ \text{ in } x, y \in \mathbb{Z} \tag{7.12}$$

has only finitely many solutions if $[K : \mathbb{Q}] \geqslant 3$ (for then $F(X, 1)$ has at least three distinct zeros and Thue's Theorem applies) or if K is an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-a})$ with a a positive integer (then $F(X, Y)$ is a quadratic form with negative discriminant and the solutions represent points with integer coordinates on an ellipsis). Equation (7.12) may have infinitely many solutions if K is real quadratic. For instance if $K = \mathbb{Q}(\sqrt{a})$ with a a positive, non-square integer, then the Pell equation $x^2 - ay^2 = N_{K/\mathbb{Q}}(x - \sqrt{a} y) = 1$ has infinitely many solutions.

We consider a generalization of (7.12) involving norm forms in an arbitrary number of variables. Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree d. Then the monic minimal polynomial f_θ of θ can be expressed as $f_\theta = \prod_{i=1}^{d} (X - \theta^{(i)})$, where $\theta^{(1)}, \ldots, \theta^{(d)} \in \mathbb{C}$ are the conjugates of θ. The embeddings of K in $\mathbb{C}$ are given by $\sigma_i(\theta) = \theta^{(i)}$ for $i = 1, \ldots, d$. Define $G := \mathbb{Q}(\theta^{(1)}, \ldots, \theta^{(d)})$. Then G is a normal number field. Denote by $\mathrm{Gal}(G/\mathbb{Q})$ the Galois group, i.e., the group of automorphisms of G. The invariant field of $\mathrm{Gal}(G/\mathbb{Q})$ is $\{\alpha \in G : \tau(\alpha) = \alpha \ \forall \tau \in \mathrm{Gal}(G/\mathbb{Q})\} = \mathbb{Q}$. Recall that each $\tau \in \mathrm{Gal}(G/\mathbb{Q})$ permutes $\theta^{(1)}, \ldots, \theta^{(d)}$. On the other hand τ is uniquely determined by its images on $\theta^{(1)}, \ldots, \theta^{(d)}$. Hence each $\tau \in \mathrm{Gal}(G/\mathbb{Q})$ may be identified with a permutation of $\theta^{(1)}, \ldots, \theta^{(d)}$, and thus

$\mathrm{Gal}(G/\mathbb{Q})$ is isomorphic to a subgroup of S_d (that is the permutation group on d elements).

Now suppose that $2 \leqslant n \leqslant d$ and let $\alpha_1, \ldots, \alpha_n$ be elements of K that are linearly independent over $\mathbb{Q}$. Define the polynomial

$$F(X_1, \ldots, X_n) := N_{K/\mathbb{Q}}(\alpha_1 X_1 + \cdots + \alpha_n X_n) := \prod_{i=1}^{d} (\sigma_i(\alpha_1) X_1 + \cdots + \sigma_i(\alpha_n) X_n).$$

Notice that if we apply any τ from the Galois group $\mathrm{Gal}(G/\mathbb{Q})$, then it permutes the linear factors of F, hence it leaves the coefficients of F unchanged. So F has its coefficients in $\mathbb{Q}$.

We deal with the so-called *norm form equation*

$$N_{K/\mathbb{Q}}(\alpha_1 x_1 + \cdots + \alpha_n x_n) = c \quad \text{in } \mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n. \tag{7.13}$$

In 1972, Schmidt gave a necessary and sufficient condition such that (7.13) has only finitely many solutions. His proof was based on the Subspace Theorem. Here, we prove a special case of his result.

Theorem 7.9. *Suppose that $n < d$, and let $\alpha_1, \ldots, \alpha_n$ be elements of K that are linearly independent over $\mathbb{Q}$. Assume that* $\mathrm{Gal}(G/\mathbb{Q}) \cong S_d$. *Then* (7.13) *has only finitely many solutions.*

We need some lemmas.

Lemma 7.10. *The vectors $(\sigma_1(\alpha_i), \ldots, \sigma_d(\alpha_i))$ $(i = 1, \ldots, n)$ are linearly independent in $\mathbb{C}^d$.*

Proof. In general, any linearly independent subset of a finite dimensional vector space can be augmented to a basis of that space. In particular, we can augment $\{\alpha_1, \ldots, \alpha_n\}$ to a $\mathbb{Q}$-basis $\{\alpha_1, \ldots, \alpha_d\}$ of K. As a consequence, there are $b_{ij} \in \mathbb{Q}$ such that

$$\theta^i = \sum_{j=1}^{d} b_{ij} \alpha_j \quad \text{for } i = 0, \ldots, d-1.$$

Then also, $\sigma_i(\theta)^j = \sum_{k=0}^{d-1} b_{jk} \sigma_i(\alpha_k)$ for $i = 1, \ldots, d$, $j = 0, \ldots, d-1$, and this leads to a matrix identity and determinant identity

$$\Big(\sigma_i(\theta)^j\Big) = \Big(\sigma_i(\alpha_j)\Big) \cdot \Big(b_{ij}\Big)^T, \quad \det \Big(\sigma_i(\theta)^j\Big) = \det \Big(\sigma_i(\alpha_j)\Big) \cdot \det \Big(b_{ij}\Big).$$

By Vandermonde's identity we have

$$\det\Big(\sigma_i(\theta)^j\Big) = \prod_{1\leqslant i<j\leqslant d} (\theta^{(j)} - \theta^{(i)}) \neq 0.$$

Hence $\det\Big(\sigma_i(\alpha_j)\Big) \neq 0$, and so the vectors $(\sigma_1(\alpha_i), \dots, \sigma_d(\alpha_i))$ $(i = 1, \dots, d)$ are linearly independent in $\mathbb{C}^d$. $\square$

Lemma 7.11. *Let $L_i := \sigma_i(\alpha_1)X_1 + \cdots + \sigma_i(\alpha_n)X_n$ for $i = 1, \dots, d$. Then the linear forms $L_1, \dots, L_d$ are in general position.*

Proof. Lemma 7.10 implies that the matrix

$$\begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & & \vdots \\ \sigma_d(\alpha_1) & \cdots & \sigma_d(\alpha_n) \end{pmatrix}$$

has column rank n. Then the row rank of this matrix is also n, which implies that this matrix has n linearly independent rows. Suppose that the rows with indices $i_1, \dots, i_n$ are linearly independent. This means precisely that the linear forms $L_{i_1}, \dots, L_{i_n}$ are linearly independent, i.e., $\det(L_{i_1}, \dots, L_{i_n}) \neq 0$.

Let $(j_1, \dots, j_n)$ be any other n-tuple of n distinct indices from $\{1, \dots, d\}$. We have to show that also $L_{j_1}, \dots, L_{j_n}$ are linearly independent, i.e., $\det(L_{j_1}, \dots, L_{j_n}) \neq 0$. The assumption that $\mathrm{Gal}(G/\mathbb{Q}) \cong S_d$ means that if we let act $\mathrm{Gal}(G/\mathbb{Q})$ on $(\theta^{(1)}, \dots, \theta^{(d)})$ we obtain all permutations of $(\theta^{(1)}, \dots, \theta^{(d)})$. In particular, there is $\tau \in \mathrm{Gal}(G/\mathbb{Q})$ such that

$$\tau(\theta^{(i_1)}) = \theta^{(j_1)}, \dots, \tau(\theta^{(i_n)}) = \theta^{(j_n)}.$$

This implies $\tau \circ \sigma_{i_1} = \sigma_{j_1}, \dots, \tau \circ \sigma_{i_n} = \sigma_{j_n}$, and consequently, that τ maps the coefficients of L_{i_k} to those of L_{j_k} for $k = 1, \dots, n$. It follows that indeed

$$\det(L_{j_1}, \dots, L_{j_n}) = \tau(\det(L_{i_1}, \dots, L_{i_n})) \neq 0.$$

$\square$

Proof of Theorem 7.9. We proceed by induction on the number of variables n. First let $n = 1$. Then equation (7.13) becomes

$$N_{K/\mathbb{Q}}(\alpha_1 x_1) = N_{K/\mathbb{Q}}(\alpha) x_1^d = c,$$

and this clearly has only finitely many solutions.

Next, let $n \geqslant 2$, and assume the theorem is true for norm form equations in fewer than n unknowns. Since $d > n$ and the linear forms $L_1, \ldots, L_d$ are in general position, we can apply Theorem 7.4, and deduce that for any $C > 0, \delta > 0$ the set of solutions of

$$|F(\mathbf{x})| = |L_1(\mathbf{x}) \cdots L_d(\mathbf{x})| \leqslant C\|\mathbf{x}\|^{d-n-\delta}$$

lies in a union of finitely many proper linear subspaces of $\mathbb{Q}^n$. It follows that the solutions of (7.13) lie in only finitely many proper linear subspaces of $\mathbb{Q}^n$.

We show that (7.13) has only finitely many solutions in each of these subspaces. Let T be one of these subspaces. For solutions in T, one of the coordinates can be expressed as a linear combination of the others, with coefficients in $\mathbb{Q}$. Say that we have $x_n = a_1x_1 + \cdots + a_{n-1}x_{n-1}$ identically on T, where $a_i \in \mathbb{Q}$. By substituting this in (7.13) we get a norm form equation in $n-1$ variables

$$N_{K/\mathbb{Q}}(\beta_1x_1 + \cdots + \beta_{n-1}x_{n-1}) = c,$$

where $\beta_i = \alpha_i + a_i\alpha_n$ for $i = 1, \ldots, n-1$. It is not difficult to show that $\beta_1, \ldots, \beta_{n-1}$ are linearly independent over $\mathbb{Q}$. Hence by the induction hypothesis, this last equation has only finitely many solutions $(x_1, \ldots, x_{n-1}) \in \mathbb{Z}^{n-1}$. This implies that the original equation (7.13) has only finitely many solutions $(x_1, \ldots, x_n) \in T$. This completes our proof. $\square$

We give examples of norm form equations with infinitely many solutions. We recall the following fact:

Lemma 7.12. *Let K be an algebraic number field and α an element of the ring of integers O_K of K. Then*

$$\alpha \textit{ is a unit of } O_K \iff N_{K/\mathbb{Q}}(\alpha) = \pm 1.$$

Proof. See Chapter 3 or Chapter 5. $\square$

It is more convenient to rewrite (7.13) as

$$N_{K/\mathbb{Q}}(\xi) = c \text{ in } \xi \in \mathcal{M}, \tag{7.14}$$

where

$$\mathcal{M} := \{\alpha_1x_1 + \cdots + \alpha_nx_n : x_1, \ldots, x_n \in \mathbb{Z}\}.$$

Notice that $\mathcal{M}$ is a free $\mathbb{Z}$-module in K of rank n, i.e., its elements can be expressed uniquely as $\mathbb{Z}$-linear combinations of a basis of n elements.

Recall that if K is a number field of degree d, having r_1 real embeddings and r_2 conjugate pairs of complex embeddings, then $r_1 + 2r_2 = d$, and by Dirichlet's Unit Theorem, the unit group O_K^* of the ring of integers of K is isomorphic to $U_K \times \mathbb{Z}^{r_1+r_2-1}$, where U_K is the finite group of roots of unity in K. This shows that O_K^* is finite if and only if $r_1 = 1$, $r_2 = 0$, in which case $K = \mathbb{Q}$, or $r_1 = 0$, $r_2 = 1$, in which case K is imaginary quadratic, i.e., of the form $\mathbb{Q}(\sqrt{-a})$ with a a positive integer.

Take an algebraic number field K such that O_K^* is infinite, i.e., $K \neq \mathbb{Q}$ and K is not imaginary quadratic. Take $\mathcal{M} = O_K$. It is known that O_K is a free $\mathbb{Z}$-module of rank equal to $[K : \mathbb{Q}]$. Now clearly, if $\varepsilon \in O_K^*$, then $\xi = \varepsilon^2$ is a solution to

$$N_{K/\mathbb{Q}}(\xi) = 1 \ \text{ in } \xi \in O_K,$$

and so this last norm form equation has infinitely many solutions.

More generally, (7.14) has infinitely many solutions if

$$\mu O_L = \{\mu\xi : \xi \in O_L\} \subseteq \mathcal{M}$$

for some $\mu \in K^*$, and some subfield L of K which is not equal to $\mathbb{Q}$ or to an imaginary quadratic field. Now Schmidt's result on norm form equations is as follows.

Theorem 7.13. (W.M. Schmidt, 1972) *Let K be an algebraic number field, $\alpha_1, \ldots, \alpha_n$ elements of K which are linearly independent over $\mathbb{Q}$, and $\mathcal{M} := \left\{ \sum_{i=1}^n \alpha_i x_i : x_i \in \mathbb{Z} \right\}$. Then the following two assertions are equivalent:*

(i) there do not exist $\mu \in K^*$ and a subfield L of K not equal to $\mathbb{Q}$ or to an imaginary quadratic field such that $\mu O_L \subseteq \mathcal{M}$;

(ii) for every $c \in \mathbb{Q}^*$, the equation

$$N_{K/\mathbb{Q}}(\xi) = c \ \ \text{in } \xi \in \mathcal{M} \tag{7.14}$$

has only finitely many solutions.

The implication (i)$\Longrightarrow$(ii) is deduced from the Subspace Theorem. The proof is too difficult to be included here. We prove only the other implication, that is, if (i) is false then there is $c \in \mathbb{Q}^*$ such that (7.14) has infinitely many solutions. Indeed, suppose that there do exist μ, L as in (i) with $\mu O_L \subseteq \mathcal{M}$. Then for every $\varepsilon \in \mathcal{O}_L^*$ we have $\mu\varepsilon^2 \in \mathcal{M}$ and $N_{K/\mathbb{Q}}(\varepsilon) = \pm 1$. Thus, by letting ε run through O_L^*, we obtain infinitely many elements $\xi = \mu\varepsilon^2 \in \mathcal{M}$ with

$$N_{K/\mathbb{Q}}(\xi) = N_{K/\mathbb{Q}}(\mu) N_{K/\mathbb{Q}}(\varepsilon)^2 = N_{K/\mathbb{Q}}(\mu).$$

□

Example. Let

$$K = \mathbb{Q}(\sqrt[6]{2}), \quad \mathcal{M} := \{x_1 \sqrt[6]{2} + x_2 \sqrt{2} + x_3 \sqrt[6]{2}^5 \,:\, x_1, x_2, x_3 \in \mathbb{Z}\}.$$

Notice that K contains the subfield $L = \mathbb{Q}(\sqrt[3]{2})$. One can show that

$$O_L = \{x_1 + x_2\sqrt[3]{2} + x_3\sqrt[3]{4} \,:\, x_i \in \mathbb{Z}\}, \quad O_L^* = \{\pm(1 - \sqrt[3]{2})^n \,:\, n \in \mathbb{Z}\}.$$

We have $\mathcal{M} = \sqrt[6]{2} O_L$ and $N_{K/\mathbb{Q}}(1 - \sqrt[3]{2}) = 1$. Hence every $n \in \mathbb{Z}$ yields a solution $\xi := \sqrt[6]{2}(1 - \sqrt[3]{2})^n \in \mathcal{M}$ of

$$N_{K/\mathbb{Q}}(\xi) = N_{K/\mathbb{Q}}(\sqrt[6]{2}) = 2.$$

7.3 Exercises

Exercise 7.1. *(i) It has been shown that* (7.5) *has infinitely many solutions in the subspace given by $x_3 = 0$. Prove that it also has infinitely many solutions in the two subspaces given by respectively $x_1 = 0$ and $x_2 = 0$.*

(ii) Prove that every one-dimensional linear subspace of $\mathbb{Q}^3$ contains only finitely many solutions of (7.5).

(iii) Prove that the solutions of (7.5) *with $x_1x_2x_3 \neq 0$ lie in only finitely many one-dimensional linear subspaces of $\mathbb{Q}^3$ and conclude that* (7.5) *has only finitely many solutions with $x_1x_2x_3 \neq 0$.*

Hint. *The solutions of* (7.5) *lie in finitely many proper linear subspaces of $\mathbb{Q}^3$. Let T be one of these subspaces. Let $ax_1 + bx_2 + cx_3 = 0$ be a non-trivial equation vanishing identically on T, with at least one of $a, b, c \neq 0$. Since we only have to consider spaces T containing solutions with $x_1x_2x_3 \neq 0$, we may assume that at most one among a, b, c is zero. Given a solution (x_1, x_2, x_3) of* (7.5) *in $T \cap \mathbb{Z}^3$, express one of the variables x_1, x_2, x_3 as a linear combination of the two others and* *substitute this into* (7.5). *What results is an inequality in two unknowns with three linear forms in general position (you have to verify this!) to which Theorem 7.4 can be applied.*

Remark. In the above exercise you were asked to prove that inequality (7.5) has only finitely many solutions outside the three subspaces $\{x_1 = 0\}$, $\{x_2 = 0\}$, $\{x_3 = 0\}$. This provides of course more precise information than the Subspace Theorem, which only gives that the solutions lie in a union of finitely many proper linear subspaces of $\mathbb{Q}^n$. Exercise 7.1 may be viewed as a special case of the following refinement of Theorem 7.4, proved by Vojta in 1989 (you are not allowed to use this in exercises although probably it wouldn't have been of any help anyway):

Theorem 7.14. *Let*

$$L_i = \alpha_{i1}X_1 + \cdots + \alpha_{in}X_n \quad (i = 1, \ldots, r,\ r \geqslant n)$$

be r linear forms with coefficients in $\overline{\mathbb{Q}}$ in general position. Then there is a finite, effectively computable, collection $U_1, \ldots, U_s$ of proper linear subspaces of $\mathbb{Q}^n$, depending only on $L_1, \ldots, L_r$, such that for every $C > 0, \delta > 0$ the following holds: the inequality

$$|L_1(\mathbf{x}) \cdots L_r(\mathbf{x})| \leqslant C \cdot \|\mathbf{x}\|^{r-n-\delta} \text{ in } \mathbf{x} \in \mathbb{Z}^n$$

has only finitely many solutions outside $U_1 \cup \cdots \cup U_s$.

The subspaces $U_1, \ldots, U_s$ remain fixed if we vary C and δ, but the finite set outside $U_1 \cup \cdots \cup U_s$ may vary with C and δ. The spaces $U_1, \ldots, U_s$ can be determined effectively in principle, but in general this may be quite hard. With the presently available proofs, the finite set of solutions outside these spaces cannot be determined effectively.

Exercise 7.2. *Let $L_1 = \alpha_1X_1 + \cdots + \alpha_nX_n$, $L_2 = \beta_1X_1 + \cdots + \beta_nX_n$ be two linearly independent linear forms with algebraic coefficients from $\mathbb{C}$.*

(i) Let $\delta > 0$, $C_1 > 0$ $C_2 > 0$. Prove that the system of inequalities

$$0 < |L_1(\mathbf{x})| \leqslant C_1\|\mathbf{x}\|^{1-n},\ 0 < |L_2(\mathbf{x})| \leqslant C_2\|\mathbf{x}\|^{1-\delta} \text{ in } \mathbf{x} \in \mathbb{Z}^n$$

has only finitely many solutions.

Hint. *Show that L_1, L_2 can be augmented to a system of n linearly independent* *linear forms by choosing $n-2$ linear forms from $X_1, \dots, X_n$.*

(ii) Assume that $\alpha_1, \dots, \alpha_n$ are linearly independent over $\mathbb{Q}$ and also that $\beta_1, \dots, \beta_n$ are linearly independent over $\mathbb{Q}$. Prove that for every $\delta > 0$ there is $C > 0$ such that the inequality

$$0 < \left| \frac{L_1(\mathbf{x})}{L_2(\mathbf{x})} \right| \leqslant C \|\mathbf{x}\|^{-n+\delta} \quad \textit{in } \mathbf{x} \in \mathbb{Z}^n$$

has infinitely many solutions.

(iii) Prove that for every $\delta > 0$ and $C > 0$, the inequality

$$0 < \left| \frac{L_1(\mathbf{x})}{L_2(\mathbf{x})} \right| \leqslant C \|\mathbf{x}\|^{-n-\delta} \quad \textit{in } \mathbf{x} \in \mathbb{Z}^n$$

has only finitely many solutions.

Remark. It is an open problem whether the boundary case

$$0 < \left| \frac{L_1(\mathbf{x})}{L_2(\mathbf{x})} \right| \leqslant C \|\mathbf{x}\|^{-n} \quad \text{in } \mathbf{x} \in \mathbb{Z}^n$$

has finitely or infinitely many solutions.

Exercise 7.3. *In this exercise you are asked to prove another generalization of Roth's Theorem. Let $C > 0, \delta > 0$, and let $\alpha_1, \dots, \alpha_n$ be real algebraic numbers such that*

$$1, \alpha_1, \dots, \alpha_n \textit{ are linearly independent over } \mathbb{Q}. \tag{7.15}$$

Consider the system of inequalities

$$|x_1 - \alpha_1 x_{n+1}| \leqslant C \|\mathbf{x}\|^{-\frac{1}{n}-\delta}, \dots, |x_n - \alpha_n x_{n+1}| \leqslant C \|\mathbf{x}\|^{-\frac{1}{n}-\delta} \tag{7.16}$$

to be solved simultaneously in $\mathbf{x} = (x_1, \dots, x_{n+1}) \in \mathbb{Z}^{n+1} \setminus \{\mathbf{0}\}$. Prove that (7.16) *has only finitely many solutions.*

Hint. *First apply the Subspace Theorem to conclude that the solutions of* (7.16) *lie in a union $T_1 \cup \dots \cup T_t$ of finitely many proper linear subspaces of $\mathbb{Q}^{n+1}$. Then show that if T is any proper linear subspace of $\mathbb{Q}^{n+1}$, then* (7.16) *has only finitely many solutions $\mathbf{x} = (x_1, \dots, x_{n+1}) \in \mathbb{Z}^{n+1} \setminus \{0\}$ inside T. There is no obvious way to do this with the Subspace Theorem, so you have to prove this directly. Take an equation $a_1 x_1 + \dots + a_{n+1} x_{n+1} = 0$ of T, with $a_1, \dots, a_{n+1} \in \mathbb{Z}$, not all 0 and use that x_i is very close to $\alpha_i x_{n+1}$ for $i = 1, \dots, n$. Assumption* (7.15) *is crucial here.*

Exercise 7.4. *Let $K = \mathbb{Q}(\sqrt[5]{2})$. Note that the embeddings of K in $\mathbb{C}$ are given by $\sigma_i(\sqrt[5]{2}) = \rho^i\sqrt[5]{2}$ for $i = 0, \dots, 4$, where $\rho = e^{2\pi\sqrt{-1}/5}$. Let $c \in \mathbb{Q}^*$, and consider the norm form equation*

$$(7.17)\quad N_{K/\mathbb{Q}}(x_1+\sqrt[5]{2}x_2+\sqrt[5]{4}x_3) = \prod_{i=0}^{4}(x_1+\rho^i\sqrt[5]{2}x_2+\rho^{2i}\sqrt[5]{4}x_3) = c \ \text{ in } x_1, x_2, x_3 \in \mathbb{Z}.$$

We observe here that the normal closure of K is $L = \mathbb{Q}(\sqrt[5]{2}, \rho)$ and that the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ *is* not *isomorphic to S_5 (in fact, it is a group of order* 20*). So Theorem 7.9 is* not *applicable. Similarly, Lemma 7.11 is not applicable.*

(i) Prove that the linear forms in the product on the right-hand side of (7.17) *are in general position.*

(ii) Prove that if $\alpha, \beta \in K^*$ and $\frac{\beta}{\alpha} \notin \mathbb{Q}$, then the linear forms $\sigma_i(\alpha)X_1 + \sigma_i(\beta)X_2$ ($i = 0, \dots, 4$) are in general position.

(iii) Prove that (7.17) *has only finitely many solutions (you are allowed to apply (i), (ii) and Theorem 7.4 but not Theorem 7.13).*

Exercise 7.5. *Using Theorem 7.13, decide for each of the norm form equations below whether or not there exists c such that it has infinitely many solutions. Let $\theta := \sqrt[6]{2}$. You may use that the only subfields of $K := \mathbb{Q}(\theta)$ are $\mathbb{Q}(\theta^2)$ and $\mathbb{Q}(\theta^3)$, and that the rings of integers of these fields are $\mathbb{Z}[\theta^2]$, $\mathbb{Z}[\theta^3]$, respectively.*

(i) $N_{K/\mathbb{Q}}(x_1 + \theta x_2 + \theta^2 x_3) = c$ *in* $(x_1, x_2, x_3) \in \mathbb{Z}^3$*;*
(ii) $N_{K/\mathbb{Q}}((1+\theta)x_1 + (1+\theta^2)x_2 + (1+\theta^3)x_3 + (1+\theta^4)x_4) = c$ *in* $(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4$.