EXAMPLE SHEET 4 FOR DIOPHANTINE ANALYSIS, LENT 2026

PÉTER VARJÚ

About this example sheet:

- Please send comments and corrections to pv270@dpmms.cam.ac.uk.
- Please submit your solutions of Questions 2 and 4, by Friday 24 April at 17:00.
- The purpose of this example sheet is to complement the material of the lectures. The level of difficulty of the problems varies considerably (in a non-monotone fashion), and they are not intended to be mock exam questions.

1. The goal of this question is to prove a special case of Theorem 48 with an effective constant following an argument of Runge.

Let $d \in \mathbf{Z}_{\geq 3}$, and let $F \in \mathbf{Z}[X, Y]$ be a homogeneous polynomial of degree d without repeated factors, which is *reducible* in $\mathbf{Z}[X, Y]$. Let $G \in \mathbf{Z}[X, Y]$ be a polynomial of degree at most $d - 1$. Suppose that $P = F - G$ is irreducible in $\mathbf{Z}[X, Y]$, and for simplicity $Y \nmid F$.

In what follows you may use without proof the following statement. With

$$F(X, Y) = (X - \alpha_1 Y) \cdots (X - \alpha_d Y)$$

there is some number $R \in \mathbf{R}_{>0}$ and for each $j = 1, \ldots, d$, there is a series

$$\varphi_j(Y) = \alpha_j Y + \beta_{j,0} + \beta_{j,1} Y^{-1} + \ldots$$

such that the following holds. We have $\beta_{j,n} \in \mathbf{Q}(\alpha_j)$ for all $j = 1, \ldots, d$ and $n \in \mathbf{Z}_{\geq 0}$. The series φ_j converges for $Y \in \mathbf{C}$, $|Y| > R$. Furthermore, for all $x, y \in \mathbf{C}$ with $|y| > R$ and $P(x, y) = 0$, we have $x = \varphi_j(y)$ for some j. (That is, $(\varphi_j(y), y)$ for $j = 1, \ldots, d$ are parametrizations of the complex solutions of $P(x, y) = 0$ for large $|y|$.)

(a) Prove that for each $j = 1, \ldots, d$, there is a polynomial $Q_j(X, Y) \in \mathbf{Z}[X, Y]$ of degree at most $[\mathbf{Q}(\alpha_j) : \mathbf{Q}]$ in the X variable such that

$$Q_j(\varphi_j(Y), Y) = \gamma_{j,1} Y^{-1} + \gamma_{j,2} Y^{-2} + \ldots$$

for some $\gamma_{j,n} \in \mathbf{C}$.

(b) Prove that for all $x, y \in \mathbf{Z}$ with $|y| > R$ and $P(x, y) = 0$, we have $Q_j(x, y) = 0$ for some $j = 1, \ldots, d$.

(c) Prove that for all $x, y \in \mathbf{Z}$ with $P(x, y) = 0$, we have $|x| + |y| < C$ for some effective constant depending only on P.

Comment: The fact that

$$X = \alpha_j Y + \beta_{j,0} + \beta_{j,1} Y^{-1} + \ldots + \beta_{j,n} Y^{-n} + O(Y^{-n-1})$$

for large solutions of $P(X,Y) = 0$ for some j and $\beta_{j,k} \in \mathbf{Q}(\alpha_j)$, where n can be taken arbitrarily large may be proved following the proof of Lemma 50. This weaker fact is, in fact, enough to solve the question. The convergence of the resulting series requires another proof. One way to do this is contained in Lemmata 4.4 and 4.5 in the book of Masser (reference [9] in the notes.)

Hint: (a) Write up the conditions to be satisfied as a system of linear equations for the coefficients of the polynomial Q_j. If the degree in Y is large enough, you should have more variables than linear constraints over $\mathbf{Q}$. (b) Prove that $Q_j(x,y)$ is an integer with absolute value less than 1. (c) Use what you know about the degrees of P and Q_j in X, and finish the argument as in the proof of Theorem 48.

Solution

(a) Fix a suitable number $D \in \mathbf{Z}_{>0}$, and consider

$$Q(X,Y) = \sum_{k=0}^{\deg \alpha_j} \sum_{l=0}^{D} a_{k,l} X^k Y^l.$$

Then expanding $\varphi_j(Y)^k$ for each k and collecting the powers of Y, we can write

$$Q(\varphi_j(Y), Y) = \sum_{i=\deg(\alpha_j)+D}^{-\infty} L_i(a_{k,l}) Y^j,$$

where $L_i(a_{k,l})$ is a linear form in the variables $a_{k,l}$ with coefficients in the field $\mathbf{Q}(\alpha_j)$. We consider the equations $L_i(a_{k,l}) = 0$ for $i = 0, \ldots, \deg(\alpha_j)D$ We have $\deg(\alpha_j) + D + 1$ linear constraints over $\mathbf{Q}(\alpha_j)$, which is equivalent to $\deg(\alpha_j)D + \deg(\alpha_j)(\deg(\alpha_j)+1)$ constraints over $\mathbf{Z}$. The number of variables is $(\deg \alpha_j + 1)(D+1)$ and this exceeds the number of variables as long as $D \geq \deg(\alpha_j)^2$, and then we can find a non-zero solution.

(b) By the property given to us in the question, $P(x,y) = 0$ and that y is sufficiently large implies $x = \varphi_j(y)$ for some j. By the previous part, we have

$$|Q_j(x,y)| = |Q_j(\varphi_j(y), y)| \leq C|y|^{-1}$$

for a suitable effective C depending only on j. (To find C, we need to find the coefficients of Q_j, which amounts to solving a system of linear equations.) Since the coefficients of Q_j are integers and $x, y \in \mathbf{Z}$, we have $Q_j(x,y) = 0$ provided $|y| > C$ for the above constant.

(c) Note that $P \nmid Q_j$, because Q_j has degree lower than P in the X variable. This is where we use that F is reducible. If P and Q_j have no common factors in $\overline{\mathbf{Q}}[X, Y]$, the effective bound on their common solutions follows by Lemma 55. If they have a common factor, then P is not irreducible over $\overline{\mathbf{Q}}$, then we can use the argument at the end of the proof of Theorem 48 using Lemma 55 again, which is again effective.

2.

(a) Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be non-zero algebraic numbers, and let K be a number field. Prove that there is a finite set $A \subset \mathcal{O}_K^\times$ depending only on $\alpha_1, \ldots, \alpha_n$ and K such that all solutions $(x_1, \ldots, x_n) \in (\mathcal{O}_K^\times)^n$ of the generalized unit equation

$$\alpha_1 x_1 + \ldots + \alpha_n x_n = 0$$

satisfies that $x_i/x_j \in A$ for some $i \neq j$.

(b) In the setting of the previous part, prove that there is a finite set $A \subset \mathcal{O}_K^\times$ depending only on $\alpha_1, \ldots, \alpha_n$ and K such that for all solutions $(x_1, \ldots, x_n) \in (\mathcal{O}_K^\times)^n$ of the above equation, the index set $\{1, \ldots, n\}$ may be partitioned as $I_1 \cup \cdots \cup I_k$ such that $x_i/x_j \in A$ whenever $i, j \in I_l$ for some $l = 1, \ldots, k$ and

$$\sum_{j \in I_l} \alpha_j x_j = 0$$

for all $l = 1, \ldots, k$.

Hint: For (a) use an argument similar to the proof of Proposition 58 from the lectures but use Theorem 60 with the set of infinite places of K as S. For (b) use (a) to show that $x_j = \beta x_i$ for some $\beta \in A$ and some $i \neq j$. Then use this to eliminate x_j and reduce to an equation in $n - 1$ variables.

Solution

(a) If $n = 2$, the claim holds with $A = \{-\alpha_2/\alpha_1\}$. We assume $n > 2$ and that the claim holds for lower values of n.
We set up an application of the subspace theorem in the form of Theorem 60. Let $V = \overline{\mathbf{Q}}^{n-1}$, and write $X_1, \ldots, X_{n-1}$ for the standard basis of V^* We consider S to be the set of infinite places of K. For each $v \in S$, we let $\Lambda_1^{(v)}, \ldots, \Lambda_{n-1}^{(v)}$ to be a subset of

$$X_1, \ldots, X_{n-1}, -\Big(\frac{\alpha_1}{\alpha_n} X_1 + \ldots + \frac{\alpha_{n-1}}{\alpha_n} X_{n-1}\Big) \tag{1}$$

and let $\Lambda_j^{(0)} = X_j$ for concreteness. There are finitely many choices for $\Lambda_j^{(v)}$, and let $\varphi_1, \ldots, \varphi_m \in V^*$ be the collection of all

functionals that arise from the applications of Theorem 60 with all of these choices.
Now let $x_1, \dots, x_n \in \mathcal{O}_K^\times$ be a solution of $\alpha_1 x_1 + \ldots + \alpha_n x_n$. There is no harm in assuming that $x_n = 1$. If we divide over by x_n the assumptions and the conclusions all remain unchanged. We first note that $\Lambda_j^{(0)}(x_1, \dots, x_{n-1}) \in \mathcal{O}_K$ and

$$\begin{aligned} &H(\Lambda_j^{(0)}(x_1, \dots, x_{n-1}) : j = 1, \dots, n-1) \\ &= \prod_{v \in M_K} \max(1, |x_1|_v, \dots, |x_{n-1}|_v)^{d_v/[K:\mathbf{Q}]} \\ &= \prod_{v \in M_K} \max_j (|x_j|_v)^{d_v/[K:\mathbf{Q}]}. \end{aligned}$$

Since $x_j \in \mathcal{O}_K^\times$ are units, $|x_j|_v = 1$ for every finite place v, so it is enough to consider the places in S in the above product.
Now fix some $v \in S$ and note that there is a choice of the $\Lambda_j^{(v)}$ such that

$$\prod_j |\Lambda_j^{(v)}(x_1, \dots, x_{n-1})|_v = \frac{\prod_j |x_j|_v}{\max_j |x_j|_v}.$$

To see this, note that the last option among the functionals evaluates to x_n on $x_1, \dots, x_{n-1}$, and one option for the choice of the functionals is to omit one that gives the largest absolute value. If we make the choice for each v that realises the above identity, we get

$$\prod_{v \in S} \prod_j |\Lambda_j^{(v)}(x_1, \dots, x_{n-1})|_v^{d_v} = \prod_v \frac{\prod_j |x_j|_v^{d_v}}{\max_j |x_j|_v^{d_v}}.$$

Since $|x_j|_v = 1$ for finite places, the product formula gives

$$\begin{aligned} \prod_{v \in S} \prod_j |\Lambda_j^{(v)}(x_1, \dots, x_{n-1})|_v^{d_v} &= \frac{1}{\prod_v \max_j |x_j|_v^{d_v}} \\ &= H(\Lambda_j^{(0)}(x_1, \dots, x_{n-1}) : j = 1, \dots, n-1)^{-[K:\mathbf{Q}]}. \end{aligned}$$

Therefore, the subspace theorem applies with this choice of the functionals, and hence $\varphi_i(x_1, \dots, x_{n-1}) = 0$ for some i. Now note that this is an equation of the form considered in the question with n reduced by 1, so we are done by the induction hypothesis.
(b) If $n = 2$, the claim follows by Part (a). Suppose $n > 2$ and that the claim holds for smaller n. Applying Part (a), there is a finite set A_0 depending only on the equation such that for all solution $x_1, \dots, x_n$ of the equation, there are $i \neq j$ and $\beta \in A_0$ such that $x_i = \beta x_j$. For simplicity of notation, we assume $i = n$ and $j = n - 1$.

We consider two cases. The first is $\beta\alpha_n + \alpha_{n-1} = 0$. In this case,

$$\alpha_{n-1}x_{n-1} + \alpha_n x_n = \alpha_{n-1}x_{n-1} + \alpha_n\beta x_{n-1} = 0.$$

We apply the induction hypothesis for the equation

$$\alpha_1 x_1 + \ldots + \alpha_{n-2}x_{n-2} = 0,$$

which yields a finite set A_1 and a partition $I_1 \cup \cdots \cup I_k$ of $1, \ldots, n-2$ such that the claimed properties hold. We take $A = \{\beta, \beta^{-1} : \beta \in A_0\} \cup A_1$ and $I_{k+1} = \{n-1, n\}$, and observe that the claimed properties hold for this A and the partition $I_1 \cup \ldots \cup I_{k+1}$, and this completes the proof in this case.
The second case is $\beta\alpha_n + \alpha_{n-1} \neq 0$. In this case, we apply the induction hypothesis for the equation

$$\alpha_1 x_1 + \ldots + \alpha_{n-2}x_{n-2} + (\alpha_{n-1} + \beta\alpha_n)x_{n-1} = 0,$$

which yields a finite set A_1 and a partition $I_1 \cup \cdots \cup I_k$ of $1, \ldots, n-2$ such that the claimed properties hold. Without loss of generality $n-1 \in I_k$. We write $\widetilde{I_k} = I_k \cup \{n\}$, and observe that the claim holds for

$$A := \{\beta^{\pm 1} : \beta \in A_0\} \cup A_1 \cup \{\beta_0^{\pm 1}\beta_1 : \beta_0 \in A_0, \beta_1 \in A_1\}$$

and the partition $I_1, \ldots, I_{k-1}, \widetilde{I_k}$.

3. Fix some $n \in \mathbf{Z}_{>1}$ and consider the vector space

$$V = \mathbf{Q}^{n^2}/\{(y, \ldots, y) : y \in \mathbf{Q}\}.$$

If $a, b \in \mathbf{Z}_{>1}$, write $e_1(a,b), \ldots, e_{n^2}(a,b)$ for an enumeration of the numbers $a^i b^j$ for $i, j = 0, \ldots, n-1$. (The enumeration is independent of a, b.)

Let $d = \gcd(a-1, b-1)$, and let $\Lambda_1, \ldots, \Lambda_{n^2-1}$ be a basis of V^* and let $v \in \{2, 3, \infty\}$. Prove that there are infinitely many choices for multiplicatively independent $a, b \in \{2^i 3^j : i, j \in \mathbf{Z}_{\geq 1}\}$ such that

$$\prod_{j=1}^{n^2-1} |\Lambda_j(e_1/d, \ldots, e_{n^2}/d)|_v > c|a|_v^{n^2(n-1)/2-n+1}|b|_v^{n^2(n-1)/2-n+1}$$

if $v = 2$ or 3 and

$$\prod_{j=1}^{n^2-1} |\Lambda_j(e_1/d, \ldots, e_{n^2}/d)|_v > c|a|_v^{n^2(n-1)/2}|b|_v^{n^2(n-1)/2}d^{-n^2+1}$$

if $v = \infty$. Here c is a constant that depends only on the functionals and v.

Conclude that the choice of the forms used in the proof of Theorem 57 is optimal up to a multiplicative constant.

Hint: Observe that you may write each Λ_j in the form $a_1 Y_1 + \ldots + a_{n^2} Y_{n^2}$, where $a_1, \ldots, a_{n^2} \in \mathbf{Q}$ are some numbers depending on j such that $a_1 + \ldots + a_{n^2} = 0$, and $Y_1, \ldots, Y_{n^2}$ are the coordinates on $\mathbf{Q}^{n^2}$. Choose a and b in such a way that $|e_1|_v, \ldots, |e_{n^2}|_v$ are distinct and far apart from one another depending on the size of the coefficients of the Λ_j in the above representation.

Solution

We can take, for example $a = 2^{N^2}3^{N^2}$ and $b = 2^N 3^{N+1}$, where N is sufficiently large depending only on functionals. These are multiplicatively independent because (N^2, N^2) and $(N, N+1)$ are linearly independent. Fix some j and write $\Lambda_j = a_1 Y_1 + \ldots + a_{n^2} Y_{n^2}$ as suggested by the hint. Let $i_{\max}$ be the index for which $|e_i|_v$ is maximal among the indices for which $a_i \neq 0$. Then we have

$$|\Lambda_j(e_1/d, \ldots, e_{n^2}/d)|_v \geq (\min_{i:a_i \neq 0} |a_i|_v)|e_{i_{\max}}/d|_v - n^2(\max |a_i|_v) \max_{i:a_i \neq 0, i \neq i_{\max}} |e_i/d|_v$$

by the triangle inequality.
We show that

$$|e_{i_{\max}}|_v > 2n^2 \frac{\max |a_i|_v}{\min_{i:a_i \neq 0} |a_i|_v} \max_{i:a_i \neq 0, i \neq i_{\max}} |e_i|_v$$

provided N is sufficiently large. Then we conclude that

$$\Lambda_j(e_1/d, \ldots, e_{n^2}/d) > c \max_{i:a_i \neq 0} |e_i/d|_v \tag{2}$$

for a certain constant c depending only on Λ_j.
To show the claim, write $e_{i_{\max}} = a^l b^k$ and write $e_{i_{\text{next}}} = a^{\widetilde{l}} b^{\widetilde{k}}$ for an index i_{next} for which the maximum in $\{i : a_i \neq 0, i \neq i_{\max}\}$ is realized. We will only use that $|a^{\widetilde{l}} b^{\widetilde{k}}|_v \leq |a^l b^k|_v$ and $(\widetilde{l}, \widetilde{k}) \neq (l, k)$. We do this with $v = \infty$ for concreteness, but the other cases are very similar.
First, suppose that $\widetilde{l} = l$. In this case

$$\frac{e_{i_{\max}}}{e_{i_{\text{next}}}} = b^{k - \widetilde{k}} \geq b,$$

and the claim holds provided N and hence b is large enough depending on Λ_j.
Second, suppose that $\widetilde{l} \neq l$. In this case

$$|\log e_{i_{\max}} - \log e_{i_{\text{next}}} - (k - \widetilde{k}) \log a| < n \log b$$

Since $\log a > n \log b$, if N is large enough, $k < \widetilde{k}$ is not compatible with $a^{\widetilde{l}} b^{\widetilde{k}} \leq a^l b^k$. We conclude

$$\frac{e_{i_{\max}}}{e_{i_{\text{next}}}} > \frac{a}{b^n},$$

and the claim holds again if N is large enough.
Now we have established (2). We fix some v, and for simplicity, we assume that $(|e_i|_v)_i$ and $(|\Lambda_j(e_1/d, \ldots, e_{n^2}/d)|_v)_j$ are both in increasing order. Considering the functionals $\Lambda_1, \ldots, \Lambda_j$, we note that at least one of them must contain some Y_i with $i > j$ with a non-zero coefficient. Indeed, if they only contained $Y_1, \ldots, Y_j$, then they would be contained in the space

$$\{a_1 Y_1 + \ldots + a_j Y_j : a_1 + \ldots + a_j = 0\},$$

which is of dimension $j - 1 < j$, and this is not possible. By (2), for the Λ_k that contains Y_i, we have

$$|\Lambda_j(\cdots)|_v \geq |\Lambda_k(\cdots)|_v > c|e_i/d|_v \geq c|e_{j+1}/d|_v,$$

where we used our monotonicity assumptions.
Multiplying these together for $j = 1, \ldots, n^2 - 1$, we get

$$\prod_{j=1}^{n^2-1} |\Lambda_j(\cdots)|_v > c^{n^2-1} \prod_{i=2}^{n^2} |e_i/d|_v.$$

Where v is finite we have $|e_i/d|_v = |e_i|_v$ and the product is missing exactly $|a^n b^n|_v$ among all $|a^k b^l|_v$. We also have $|e_i/d|_\infty = |e_i|_\infty/d$ and the product is missing exactly $|a^0 b^0/d|_v$. The claim follows by collecting the powers of $|a|_v$ and $|b|_v$ in the product.

4. Let K be a number field. Prove that there is an effective constant depending only on K such that any solution $\alpha, \beta \in \mathcal{O}_K^\times$ of

$$\alpha + \beta = 1$$

satisfies $H(\alpha), H(\beta) \leq C$.

Hint: Pick a fundamental system of units $u_1, \ldots, u_r \in \mathcal{O}_K^\times$. Prove that for all $n_1, \ldots, n_r$, there is at least one place $v \in M_{K,\infty}$ such that

$$|u_1^{n_1} \cdots u_r^{n_r}|_v > (1 + c)^{\max(|n_1|, \ldots, |n_r|)}$$

for some $c > 0$ depending only on K and the choice of $u_1, \ldots, u_r$. Use the logarithmic embedding to do this and that a vector cannot be almost orthogonal to all the coordinate axes.

Write α and β as products of roots of unity and powers of the fundamental units. Prove that if $\alpha + \beta = 1$, then $|\alpha/\beta + 1|_v$ is exponentially small in the exponents that appear in the representation of α and β for a suitable v.

Use the embedding into $\mathbf{C}$ associated to v and lower bounds for linear forms in logarithms.

Solution

We first prove the claim in the hint. We consider the logarithmic embedding

$$\Phi : K^\times \to \mathbf{R}^{M_{K,\infty}}, \qquad \Phi(\alpha) = (d_v \log |\alpha|_v)_v.$$

Since $\Phi(u_1), \dots, \Phi(u_r)$ are linearly independent, there is a constant $c > 0$ such that

$$\|n_1\Phi(u_1) + \ldots + n_r\Phi(u_r)\| > c \max(|n_1|, \dots, |n_r|).$$

If this was false, then we could find a sequence of vectors $(x_1^{(m)}, \dots, x_r^{(m)})$ such that $\max_j(|x_j^{(m)}|) = 1$ for all m and $\|x_1^{(m)}\Phi(u_1) + \ldots + x_r^{(m)}\Phi(u_r)\| \to 0$ as $m \to \infty$. Taking the limit, we get a contradiction to linear independence.
Since all norms are equivalent on a finite dimensional vector space, we can take $\|\cdot\|$ to be the maximum of the coordinates. We conclude the inequality

$$\max_{v \in M_{K,\infty}} |\log |u_1^{n_1} \cdots u_r^{n_r}|_v^{d_v}| > c \max(|n_1|, \dots, |n_r|).$$

Using the product formula in the form $\sum_v \log |u_1^{n_1} \cdots u_r^{n_r}|_v^{d_v} = 0$, we conclude that

$$\max_{v \in M_{K,\infty}} \log |u_1^{n_1} \cdots u_r^{n_r}|_v^{d_v} > \frac{c}{[K : \mathbf{Q}]} \max(|n_1|, \dots, |n_r|).$$

Exponentiating this, and adjusting the value of c, as needed, the claim follows.
We write $\alpha = \theta_1 u_1^{n_1} \cdots u_r^{n_r}$ and $\beta = \theta_2 u_1^{m_1} \cdots u_r^{m_r}$ where θ_1, θ_2 are roots of unity and n_i, m_i are integers. We assume, as we may, that $\max(|n_1|, \dots, |n_r|) \leq \max(|m_1|, \dots, |m_r|)$. Using the claim, there is an embedding $\sigma : K \to \mathbf{C}$ such that

$$|\sigma(\alpha/\beta + 1)| = |\sigma(\beta)|^{-1} < (1 + c)^{-\max(|m_1|,\dots,|m_r|)}.$$

To simplify the notation, we identify $\sigma(\alpha)$ and $\sigma(\beta)$ with α and β.
Taking logarithm of the inequality, we can write

$$\begin{aligned} |\Lambda| &:= |\log(-\theta_1/\theta_2) + (n_1 - m_1)\log u_1 + \dots \\ &\qquad + (n_r - m_r)\log u_r + 2k \log(-1)| \\ &\leq (1 + c)^{-\max(|m_1|,\dots,|m_r|)}. \end{aligned}$$

Here all of the logarithms are the principal branch, and we choose the value of k to make the imaginary part as small as possible. It is easy to see that $k \leq C \max(|n_j - m_j|)$ for a suitable constant.

Now we apply a lower bound for linear forms in logarithms. Even the simpler Theorem 16 will suffice. The numbers that we plug in as α_j are all fixed, $-\theta_1/\theta_2$, a root of unity in K, $u_1, \ldots, u_r$ and -1. Therefore, all the A parameters are bounded by an effective constant depending only on K and the choice of the fundamental units. We also have $B \leq C \max(|n_j - m_j|)$. It follows that

$$|\Lambda| \geq \exp(-C \log B) \geq \max(|n_j - m_j|)^{-\widetilde{C}} \geq \max(|m_j|)^{-\widetilde{C}}$$

for a suitable effective $\widetilde{C}$. Comparing this with our previous upper bound, we see that $\max(|m_1|, \ldots, |m_r|)$ is bounded by an effective constant depending only on K. From this the claim follows using standard height bounds.

5. Let $m \in \mathbf{Z}_{\geq 1}$ and let $\alpha_1, \ldots, \alpha_m \in \overline{\mathbf{Q}}_{\neq 0}$ be such that α_i/α_j is not a root of unity for any $1 \leq i \neq j \leq m$. Let $P_1, \ldots, P_m \in \overline{\mathbf{Q}}[X]$ be non-zero polynomials. Use the subspace theorem to prove that there are at most finitely many $n \in \mathbf{Z}$ such that

$$P_1(n)\alpha_1^n + \ldots + P_m(n)\alpha_m^n = 0.$$

Hint: It is enough to prove the finiteness for $n \in \mathbf{Z}_{\geq 0}$. Show that you may assume without loss of generality that all α_j and the coefficients of all P_j are algebraic integers. Let K be a number field containing all the α_j and all the coefficients. Let $S \subset M_K$ be finite containing all infinite places such that $|\alpha_j|_v = 1$ for all j and all $v \notin S$. Use the subspace theorem on the space

$$V = \{(x_1, \ldots, x_m) \in K^m : x_1 + \ldots + x_m = 0\}$$

and for the places S. Choose the functionals from among $\{X_1, \ldots, X_m\}$ for each $v \in S$. Prove that there is $v \in S$ such that $|\alpha_1|_v, \ldots, |\alpha_m|_v$ are not all equal.

Solution

It is enough to consider the solutions $n \geq 0$, and then the claim will follow for the solutions $n \leq 0$ after substituting $-n$ for n.
If we replace each α_j by $M\alpha_j$ and each P_j by NP_j for some integers M and N, the left hand side of the nth equation is multiplied by NM^n, so whether or not it is 0 remains unchanged. Therefore, there is no harm in assuming that each α_j and the coefficients of each P_j are algebraic integers.
We prove the claim by induction on n. If $n = 1$, then $P_1(n)\alpha_1^n = 0$ if and only if $P_1(n) = 0$, which happens only for finitely many n, so the claim holds.

Suppose that $n > 1$ and the claim holds for smaller values of n. We show that there is a place v such that not all $|\alpha_j|_v$ are equal. Suppose to the contrary that $|\alpha_1|_v = |\alpha_2|_v$ for every place v. Then $|\alpha_1/\alpha_2|_v = 1$ for all v. Since this holds for all finite places, α_1/α_2 is an algebraic integer. Since it holds for all the infinite places, it is an algebraic integer all of whose Galois conjugates lie on the unit circle. Therefore, α_1/α_2 is a root of unity by Kronecker's theorem, which is contrary to our assumption.
We apply the subspace theorem on the space

$$V = \{(x_1, \dots, x_m) \in K^m : x_1 + \dots + x_m = 0\}.$$

Let S be the set of infinite places of K and those finite places v for which $|\alpha_j|_v \neq 1$ for some j. This is a finite set. For each $v \in S$, we choose $\Lambda_1^{(v)}, \dots, \Lambda_{m-1}^{(v)} \in V^*$ to be a subset of the functionals $X_1, \dots, X_m$, which are the restrictions of the standard coordinates on K^m to V. We let $\Lambda_j^{(0)} = X_j$. We apply the subspace theorem for all possible choices of the functionals (for each place we need to decide which coordinate to drop), and denote by $\varphi_1, \dots, \varphi_l$ the union of all functionals that arise from one of theses applications of the theorem.
We evaluate the functionals on the point

$$(P_1(n)\alpha_1^n, \dots, P_m(n)\alpha_m^n),$$

which is in V if n is a solution of the equation. There is a choice of the functionals such that for a place v, we drop X_j for a j such that $|\alpha_j^n|_v$ is maximal. If we make that choice, then we have

$$\begin{aligned}\prod_{v\in S}\prod_{j=1}^{m-1} |L_j^{(v)}(P_1(n)\alpha_1^n, \dots, P_m(n)\alpha_m^n)|_v^{d_v} \\ &\leq \prod_{v\in S}\left(\prod_{j=1}^{m}\max(1, |P_j(n)|_v)^{d_v}\frac{\prod_{j=1}^m |\alpha_j^n|_v^{d_n}}{\max_j |\alpha_j^n|_v}\right) \\ &= H(P_j(n))^d H_p(\alpha_1, \dots, \alpha_m)^{-nd},\end{aligned}$$

where $d = [K : \mathbf{Q}]$.
We have seen that there is a place w such that $|\alpha_1|_v \neq |\alpha_2|_v$, say $|\alpha_2|_w > |\alpha_1|_w$. Then

$$H_p(\alpha_1, \dots, \alpha_m)^d \geq \prod_v \max(|\alpha_1|_v, |\alpha_2|_v)^{d_v} \geq \frac{|\alpha_2|_w^{d_w}}{|\alpha_1|_w^{d_w}}\prod_v |\alpha_1|_v^{d_v} > 1.$$

On the other hand, $H(P_j(n))^d$ only grows polynomially in n. It is also not hard to see that

$$H(P_1(n)\alpha_1^n, \dots, P_{m-1}(n)\alpha_{m-1}^n) < C^n$$

for some C. To see these two claims, observe that only finitely many absolute values contribute to the height, and each absolute value is bounded by a polynomial in the first case and by an exponential in the second.
Then

$$\prod_{v\in S}\prod_{j=1}^{m-1}|L_j^{(v)}(P_1(n)\alpha_1^n,\dots,P_m(n)\alpha_m^n)|_v^{d_v} \leq H(P_1(n)\alpha_1^n,\dots,P_{m-1}(n)\alpha_{m-1}^n)^{-\varepsilon}$$

for a suitable $\varepsilon > 0$ if n is large enough.
Therefore, the subspace theorem applies and we have that

$$\varphi_i(P_1(n)\alpha_1^n,\dots,P_m(n)\alpha_m^n) = 0$$

for some i. This together with $P_1(n)\alpha_1^n + \ldots + P_m(n)\alpha_m^n = 0$ implies a linear equation in $m-1$ of the terms. The induction hypothesis applied to this equation implies that this may hold for at most finitely many n.

6. In the setting of the previous question, assume that $|\alpha_1| > |\alpha_j|$ for all $j \geq 3$, but we permit $|\alpha_1| = |\alpha_2|$. (We fix an embedding into $\mathbf{C}$.) Use lower bounds for linear forms in logarithms to prove that there is an effective constant C depending only on $\alpha_1,\dots,\alpha_m$ and $P_1,\dots,P_m$ such that

$$P_1(n)\alpha_1^n + \ldots + P_m(n)\alpha_m^n \neq 0.$$

for all $|n| > C$.

Hint: Let K be as in the previous hint. If $m = 2$, show that there is a $v \in M_K$ such that $|\alpha_1|_v \neq |\alpha_2|_v$ and finish using just this without linear forms in logarithms.

If $m > 2$ and $|\alpha_1| = |\alpha_2|$, then show that

$$-\frac{P_1(n)}{P_2(n)}\Big(\frac{\alpha_1}{\alpha_2}\Big)^n$$

is very close to 1 for those n with $P_1(n)\alpha_1^n + \ldots + P_m(n)\alpha_m^n = 0$ and use lower bounds for linear forms in logarithms.

Use the $m = 2$ case to deal with the potential vanishing of your linear form in logarithms.

Solution

It is enough to consider the solutions $n \geq 0$, and then the claim will follow for the solutions $n \leq 0$ after substituting $-n$ for n.
First suppose $m = 2$. Using that α_1/α_2 is not a root of unity, there is a place v such that $|\alpha_1|_v > |\alpha_2|_v$. Note that there is constant C such that $|P_2(n)|_v \leq Cn^C$ for all n. (Indeed, choose

C to be larger than the degree and the sum of the absolute values of the coefficients of P_2.) In addition, $|P_1(n)|_v > cn^{-C}$ for some $c > 0$ and C if $P_1(n) \neq 0$, which is the case for all but finitely many n. One way to see this is to give an upper bound for $H(P_1(n))$ and then use a version of the Liouville bound. It follows that

$$|P_1(n)\alpha_1^n + P_2(n)\alpha^n|_v > cn^{-C}|\alpha_1|_v^n - Cn^C|\alpha_2|_v^n > 0$$

if n is larger than a constant that can be computed in terms of $\alpha_1, \dots, \alpha_m$, c, C and d.

Now we consider the case $m > 2$. If $|\alpha_1| \neq |\alpha_2|$, say $|\alpha_1| > |\alpha_2|$, then it is possible to prove similarly to the argument in the $m = 2$ case above that term $P_1(n)\alpha_1^n$ will dominate, so there are no solutions for large n.

Now suppose $|\alpha_1| = |\alpha_2|$. We write $a = \max_{j\geq 3}(|\alpha_j|/|\alpha_2|) < 1$. Similarly as above, $|P_i(n)| \leq C|n|^C$ for all i and n and $|P_2(n)| > c$ for suitable $c > 0$, whenever $P_2(n) \neq 0$. (In this case, it is easy to see that the leading term of the polynomial will dominate.) It follows that

$$\left| \frac{P_1(n)}{P_2(n)} \left(\frac{\alpha_1}{\alpha_2} \right)^n + 1 \right| \leq (C/c)m \cdot n^C a^n.$$

Taking logarithms, we get

$$|\Lambda| := |\log(-P_1(n)/P_2(n)) + n\log(\alpha_1/\alpha_2) + 2k\log(-1)| < Cb^n,$$

where C is another constant, and $b \in (a, 1)$. Here the logarithms are the principal branches and k is chosen in such a way to match up the sum of the logarithms with the principal branch of $\log 1$. Computing that the imaginary part of the log's are less than π in absolute value, it is easy to see that $k \leq 2n + 1$.

If $\Lambda = 0$, then necessarily $P_1(n)\alpha_1^n + P_2(n)\alpha_2^n = 0$, and we can conclude using the $m = 2$ case above.

If $\Lambda \neq 0$, then we can use the lower bound in Theorem 16 again. The A parameter corresponding to $-P_1(n)/P_2(n)$ is equal to $H(-P_1(n)/P_2(n)) \leq Cn^C$ for some constants depending on P_1 and P_2. This can be seen by repeatedly applying the bounds $H(\alpha + \beta) \leq 2H(\alpha)H(\beta)$ and $H(\alpha\beta) \leq H(\alpha)H(\beta)$ for example. The B parameter is bounded by $\max(2n + 1, \log A_1) = 2n + 1$ if n is large enough. We get

$$|\Lambda| > \exp(-\log(Cn^C)\log(2n + 1)).$$

Contrasting this with the upper bound, we get

$$\exp(-\log(Cn^C)\log(2n + 1)) < Cb^n,$$

and this yields an effective upper bound for n.

7. Let $x \in (0,1)$ be a number with base 10 digit expansion $0.x_1x_2x_3\ldots$. We say that the expansion has long repetitions if there is some $\varepsilon > 0$ and infinitely many $n \in \mathbf{Z}_{>0}$ such that $x_1x_2\ldots x_n$ contains two identical substrings of length $\lceil \varepsilon n \rceil$. That is to say, there are $1 \leq k < m \leq n-l+1$ and $l = \lceil \varepsilon n \rceil$ such that $x_{k+j} = x_{m+j}$ for $j = 0, \ldots, l-1$.

(a) Suppose that $x \in (0,1)$ has long repetitions in its base 10 digit expansion. Prove that there is $\varepsilon > 0$ and infinitely many $n \in \mathbf{Z}_{>0}$ such that there are integers $0 \leq k \neq m \leq n$ and $A \in \mathbf{Z}$ with

$$|10^m x - 10^k x - A| \leq 10^{-\varepsilon n}.$$

(b) Use the subspace theorem to show that if $x \in (0,1)$ has long repetition in its base 10 digit expansion, then x is either rational or transcendental.

Comment: This is a result of Adamczewski, Bugeaud and Luca.

Hint: (a): With k, m as in the definition of long repetitions, show that $10^{k-1}x$ and $10^{m-1}x$ are close to each other in $\mathbf{R}/\mathbf{Z}$. (b): Use $S = \{2, 5, \infty\}$. Suppose x is algebraic. Use the coordinate functions as your linear forms together with $xX_1 - xX_2 - X_3$ for $v = \infty$ and evaluate them at the point $(10^m, 10^k, A)$. Prove that if a proper linear subspace contains infinitely many solutions of the inequality in your application of the subspace theorem then it is given by the equation $xX_1 - xX_2 - X_3 = 0$. Conclude that x is rational.

Solution

(a) Let k and m be the integers so that $x_{k+j} = x_{m+j}$ for $j = 1, \ldots, l$. Then the first l digits of $10^m x$ and $10^k x$ after the decimal point are identical. That is, there are $a_1, a_2, b \in \mathbf{Z}$ and $e_1, e_2 \in \mathbf{R}$ such that $10^m x = a_1 + b/10^l + e_1$, $10^k = a_2 + b/10^l + e_2$ and $0 \leq e_1, e_2 \leq 10^{-l}$ (a_1 is the integer part of $10^m x$ and e_1 is 10^{-l} times the fractional part of $10^{m+l}x$.)
Therefore,

$$|10^m x - 10^k x - (a_1 - a_2)| \leq 10^{-l} \leq 10^{-\varepsilon n}.$$

(b) Suppose x is algebraic. Apply the subspace theorem in $\mathbf{Q}^3$ with $S = \{2, 5, \infty\}$. Set $L_j^{(v)} = X_j$ for all j and v with the exception of $L_3^{(v)} = xX_1 - xX_2 - X_3$. If we plug in $(10^m, 10^k, A)$,

we get

$$\prod_{v\in S}\prod_{j=1}^{3}|L_j^{(v)}(10^m,10^k,A)|_v$$
$$=\left(\prod_{v\in S}|10^m|_v\right)\left(\prod_{v\in S}|10^k|_v\right)|A|_2|A|_5|10^m x-10^k x-A|_\infty$$
$$\leq 10^{-\varepsilon m}.$$

By the construction in the previous part, A is the integer part of $10^m x$, hence $10^k, A \leq 10^m$ and $H(10^m, 10^k, A) \leq 10^m$. Therefore, the subspace theorem applies, and it follows that there are finitely many proper subspaces $V_1, \dots, V_t$ that depend only on x and ε but not on n, m or k such that $(10^m, 10^k, A) \in V_i$ for some i.
Since x has long repetitions, one of the subspaces must contain infinitely many solutions. Say it is V_1. Suppose that $xX_1 - xX_2 - X_3$ does not vanish on V_1. Then the restriction of $xX_1 - xX_2 - X_3$ to V_1 must be linearly independent from the either the restriction of X_1 or X_2, because the restrictions of X_1, X_2 and $xX_1 - xX_2 - X_3$ span the dual of V_1. Say X_1 and $xX_1 - xX_2 - X_3$ are linearly independent. We let $\widetilde{L}_1^{(\infty)} = X_1|_{V_1}$ and $\widetilde{L}_2^{(\infty)} = (xX_1 - xX_2 - X_3)|_{V_1}$. By a similar reasoning, the restriction of X_1 to V_1 is linearly independent from the restriction of X_2 or X_3. We let $\widetilde{L}_1^{(v)} = X_1|_{V_1}$ and $\widetilde{L}_2^{(v)} = X_2|_{V_1}$ or $\widetilde{L}_2^{(v)} = X_3|_{V_1}$ for $v = 2, 5$. The subspace theorem applies again, so we conclude that all solutions are contained in finitely many lines. As we discussed in the lectures, having infinitely many solutions on a line is possible only if one of the forms vanish on the line. Since 10^k, 10^m and A are non-zero, the only form that can vanish is $xX_1 - xX_2 - X_3$.
We conclude that all but finitely solutions of the inequality in V_1 satisfies

$$x \cdot 10^m - x \cdot 10^k - A = 0.$$

This holds whether or not this form vanishes on the entire subspace V_1. But having just one such solution, implies that $x = A/(10^m - 10^k) \in \mathbf{Q}$.
We proved that if x is algebraic, then it is rational. Therefore, it is either transcendental of rational.