EXAMPLE SHEET 2 FOR DIOPHANTINE ANALYSIS, MICHAELMAS 2024

PÉTER VARJÚ

About this example sheet:

- Please send comments and corrections to pv270@dpmms.cam.ac.uk.
- Please submit your solutions of Problems 3 *or* 4 and 9, by Monday 11 November, 13:00.
- 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. Fix some numbers $H, D \in \mathbf{Z}_{>0}$. Prove that the number of algebraic numbers α with $H(\alpha) \leq H$ and $\deg(\alpha) \leq D$ is at most $3^{D+1}D(2H)^{D(D+1)}$.

2. Prove that for every $D \in \mathbf{Z}_{>0}$, there is a constant $c = c(D)$ such that for all $H \in \mathbf{Z}_{>0}$, the number of algebraic numbers with $H(\alpha) \leq H$ and $\deg(\alpha) = D$ is at least $cH^{D(D+1)}$.

3. Fix some $H \in \mathbf{R}_{>0}$ and $d \in \mathbf{Z}_{>0}$. Let α be an algebraic number of degree at most d with

$$H(\alpha) \leq H^{1/|\{\beta \in \overline{\mathbf{Q}} : \deg(\beta) \leq d, H(\beta) \leq H\}|}.$$

Prove that α is a root of unity or $\alpha = 0$.

Choose some value of H and combine with Question 1 to get an explicit $H_0(d) > 1$ such that for a non-zero algebraic number α of degree d, $H(\alpha) < H_0(d)$ implies that α is a root of unity.

4. Let α be an algebraic number of degree d and let $D \geq d$ a rational integer. Use Siegel's lemma to find a number A such that a polynomial P with $\deg P \leq D$, $H(P) \leq A$ and $P(\alpha) = 0$ exists. (Try to make A as small as you can.) Use this to improve on the $H_0(d)$ you got in Question 3.

5. Let $P, Q \in \mathbf{Z}[X]$ with $Q|P$. Prove that

$$H(Q) \leq 2^{\deg Q}(\deg(P) + 1)H(P).$$

6. Let $a \in \mathbf{Z}_{\geq 3}$, and $d \in \mathbf{Z}_{\geq 2}$. Prove that the polynomial $X^d - aX^{d-1} + 1$ is irreducible, and it has exactly one root with absolute value greater than 1. Write α for this root. Prove that $a - 1 < \alpha < a$, $|\alpha| = M(\alpha)$ and $|\alpha^{-1}| = M(\alpha^{-1})^{-1}$. Conclude the equality in Liouville's inequality is possible for any degree.

Remark: Real algebraic integers that are greater than 1 and all of whose Galois conjugates have modulus strictly less than 1 are called Pisot or PV numbers. They have many interesting properties.

7.

(a) Let α be an algebraic number of degree d, and $p, q \in \mathbf{Z}$ with $q \neq 0$. Give an upper bound for $H(\alpha - p/q)$ and use this via Liouville's inequality to give a lower bound on $|\alpha - p/q|$.

(b) Let $\alpha_1, \ldots, \alpha_n \in \overline{\mathbf{Q}}_{\neq 0}$ and $b_1, \ldots, b_n \in \mathbf{Z}$. Give an upper bound for $H(\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1)$ and use this to show

$$|b_1 \log(\alpha_1) + \ldots + b_n \log(\alpha_n)| \geq \exp(-(D+1)\log 2 - (\log H(\alpha_1) + \ldots \log H(\alpha_n))DB),$$

where D is the degree of the number field $\mathbf{Q}(\alpha_1, \ldots, \alpha_n)$ and $B = \max(|b_1|, \ldots, |b_n|)$.

8.

(a) Let K be a number field, and let $\alpha \in K$. Consider the number

$$\beta = \alpha^5 + (1-\alpha)^5 - 1.$$

Prove that

$$|\beta|_v \leq 3 \max(1, |\alpha|_v)^5 \max(1, |1-\alpha|_v)^5$$

for all $v \in M_K$.

(b) Show that $\beta = 5P(\alpha)$ for some $P \in \mathbf{Z}[X]$ of degree 4. Use this to prove

$$|\beta|_v \leq |5|_v \max(1, |\alpha|_v)^4 \leq |5|_v \max(1, |\alpha|_v)^5 \max(1, |1-\alpha|_v)^5$$

for all $v \in M_{K,f}$.

(c) Show that

$$H(\alpha)H(1-\alpha) \geq \left(\frac{5}{3}\right)^{1/5}$$

or $\alpha \in \{0, 1, (1 \pm \sqrt{-3})/2\}$.

9. Prove that for all real irrational algebraic α and $\varepsilon > 0$, there is an effective constant $C = C(\alpha, \varepsilon)$ such that the number of pairs of integers $p, q \in \mathbf{Z}$ with $q \neq 0$, $\gcd(p, q) = 1$ such that

$$|\alpha - p/q| < C^{-1} q^{-\sqrt{2d} - \varepsilon}$$

is at most C.

10. The following statement in known as Dyson's lemma.

Lemma. *Let* $m \in \mathbf{Z}_{\geq 1}$*, and let* $x_1, \dots, x_m \in \mathbf{C}$ *and* $y_1, \dots, y_m \in \mathbf{C}$ *be two sets of distinct numbers. Let* $t_1, \dots, t_m \in [0, 1]$*. Let* $P \in \mathbf{C}[X_1, X_2]$ *be a non-zero polynomial of degree at most* n_1 *in* X_1 *and* n_2 *in* X_2*. Suppose*

$$I_P(x_j, y_j; n_1^{-1}, n_2^{-1}) \geq t_j$$

for $j = 1, \dots, m$*. Then*

$$\sum_{j=1}^{m} \frac{t_j^2}{2} \leq 1 + \max\Big(\frac{m-2}{2}, 0\Big)\frac{n_2}{n_1}.$$

For a slightly more general version of the above lemma, see [Bombieri, Acta Math. **148** (1982)].

Give a proof of Dyson's Diophantine exponent $\sqrt{2d} + \varepsilon$ (Theorem 29) using Dyson's lemma instead of the non-vanishing result in Section 3.3.

11. Fix some numbers $\varepsilon, C > 0$. Suppose that ε is smaller than a suitable absolute constant (e.g. $\varepsilon \leq 1/6$ would do). Show that there are $n_1, n_2 \in \mathbf{Z}_{\geq 1}$, $p_1/q_1, p_2/q_2 \in \mathbf{Q}$ and a polynomial $0 \neq P \in \mathbf{Z}[X_1, X_2]$ of degree at most n_1 in X_1 and n_2 in X_2 such that the following holds.

$$\exp(n_1 + n_2) \leq q_j^{n_j/C},$$
$$H(P) \leq q_j^{n_j/C}$$

for $j = 1, 2$,

$$I_P(p_1/q_1, p_2/q_2; \log q_1, \log q_2) \geq \varepsilon(n_1 \log q_1 + n_2 \log q_2)$$

and

$$\log q_2 \geq (10\varepsilon)^{-1} \log q_1.$$

It is useful to consider P of the form $(F(X_1) - G(X_1)X_2)^n$ and evaluate it at $(X_1, X_2) = (p_1/q_1, p_2/q_2)$ with $p_2/q_2 = F(p_1/q_1)/G(p_1/q_1)$ for some choice of p_1/q_1.

Compare this with the non-vanishing result in Section 3.3.