

Algebraic Number Theory 88-798  
Question Sheet 1

Please feel free to e-mail me at [mschein@math.biu.ac.il](mailto:mschein@math.biu.ac.il) with any questions of translation or otherwise.

- (1) We start with an exercise in elementary (pre-algebraic) number theory. Prove that the only solution of the equation

$$3^a - 2^b = 1$$

with  $a, b > 1$  is  $a = 2, b = 3$ .

*Hint:* Suppose that  $(a, b)$  is a solution. Show first that  $a$  must be even (by considering the equation modulo 4) and  $b$  must be odd (by considering it modulo 3).

This statement was proved by the Ralbag (Rabbi Levi ben Gershon) in the 14th century. In fact it is true that the only solution of  $x^a - y^b = 1$  for *any* positive integers  $x$  and  $y$ , with  $a, b > 1$ , is  $3^2 - 2^3 = 1$ . This general result is called Catalan's conjecture and was only proved in 2002, by Preda Mihailescu using methods of algebraic number theory considerably beyond those we will study in this course.

- (2) Let  $d$  be a square-free integer (i.e.  $d$  is not divisible by  $m^2$  for any  $m > 1$ ) such that  $d \neq 0, 1$ . Let  $K = \mathbb{Q}(\sqrt{d})$ . Show that

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & : \text{if } d \equiv 2, 3 \pmod{4} \\ \mathbb{Z}[\frac{1}{2}(1 + \sqrt{d})] & : \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

- (3) Let  $\alpha = \sqrt[4]{2}$  and  $K = \mathbb{Q}(\alpha) \subset \mathbb{C}$ . Show that  $\sqrt{3} \notin K$ .

*Hint:* Every element  $x \in K$  has the form  $x = b_0 + b_1\alpha + b_2\alpha^2 + b_3\alpha^3$  for  $b_i \in \mathbb{Q}$ . Prove that  $\text{Tr}_{K/\mathbb{Q}}(x) = 4b_0$ . Now suppose that  $\sqrt{3}$  can be expressed in this form and compute the traces of  $\sqrt{3}$  and  $\sqrt{3}/\alpha$ . Use this to derive a contradiction.

- (4) Let  $K/\mathbb{Q}$  be a number field and suppose that  $\alpha \in K$ . Prove that the following are equivalent:
- (a)  $\alpha$  is a root of a monic polynomial (פולינום מתוקן)  $f \in \mathbb{Z}[x]$ .
  - (b) The minimal polynomial  $g \in \mathbb{Q}[x]$  of  $\alpha$  is contained in  $\mathbb{Z}[x]$ . (Recall that the minimal polynomial of  $\alpha$  is the unique monic irreducible polynomial in  $\mathbb{Q}[x]$  of which  $\alpha$  is a root.

*Hint:* Prove the following. If  $f \in \mathbb{Z}[x]$  and  $g, h \in \mathbb{Q}[x]$  are monic polynomials such that  $f = gh$ , then  $g, h \in \mathbb{Z}[x]$ . Indeed, let  $m$  be the smallest positive integer such that  $mg \in \mathbb{Z}[x]$  and let  $n$  be the smallest positive integer such that  $nh \in \mathbb{Z}[x]$ . We want to show that  $m = n = 1$ . Suppose not, and let  $p$  be a prime dividing  $mn$ . Considering the equation  $mnf = (mg)(nh)$ , show that  $p$  must divide all the coefficients of either  $mg$  or  $nh$ .

- (5) Let  $R = \mathbb{Q}[x, y]$ , and let  $I$  be the ideal  $(x^2 - y^3)$ . Show that  $A = R/I$  is an integral domain (תחום שלמות), but that  $A$  is not integrally closed (סגור בשלמות).