# Algebraic Number Theory

## Problem sheet 2

In this sheet, let $K$ be a number field, i.e. a finite extension of $\mathbb{Q}$, recall that $\mathcal{O}_K$ is its ring of integer and $d_K$ is its discriminant.

1. (3 points) Let $\alpha \in \mathbb{C}$ be an algebraic number and let $f(T)$ be its minimal polynomial. Recall that $f(T) \in \mathbb{Q}[T]$. Prove that $\alpha$ is an algebraic integer if and only if $f(T) \in \mathbb{Z}[T]$.

2. (5 points) Show that $d_K \equiv 0, 1 \pmod 4$. (Hint: Try taking the permanent (ie. sum of all expression with + sign as in the determinant) of the matrix $((\sigma_i \alpha_j))$ and use the identity $(a-b)^2 = (a+b)^2 - 4ab$.)

3. (3+3 points) Let $K = \mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Z}$ is squarefree.
   (a) Find an integral basis of $\mathcal{O}_K$. Hence determine $d_K$(compare with Problem 2).
   (b) Given $p$ an odd prime such that $p \nmid d_K$. Show that $p\mathcal{O}_K$ is a prime ideal if and only if $\left(\frac{d}{p}\right) = -1$.

4. (2+2 points) Let $\omega_1, .., \omega_n$ be $n$ elements of $\mathcal{O}_K$ such that they are $\mathbb{Q}$-linearly independent. Recall the discriminant of $\omega_1, .., \omega_n$ is $d(\omega_1, .., \omega_n) := \det((\sigma_i \omega_j))^2$.
   (a) Show that the quotient $\frac{d(\omega_1, .., \omega_n)}{d_K}$ is a perfect square.
   (b) If $d(\omega_1, .., \omega_n)$ is squarefree, prove that $\omega_1, .., \omega_n$ is an integral basis. Does the converse hold?

5. (3 points) Let $K = \mathbb{Q}[\theta]$, where $\theta^3 - \theta - 4 = 0$. Prove that $1, \theta, \frac{\theta + \theta^2}{2}$ is an integral basis of $\mathcal{O}_K$.

6. (3 points) Verify that the ring $\mathbb{C}[x, y]/(y^2 - x^3)$ is not integrally closed.

7. (2 points) Let $K = \mathbb{Q}(\sqrt{-7})$. Decompose $33 + 11\sqrt{-7}$ as a product of irreducible elements in $\mathcal{O}_K$.

8. (3+3+3 points) Let $A$ be a Dedekind domain(for example $\mathcal{O}_K$).
   $(a)$ Prove that $A$ is PID if and only if $A$ is UFD
   $(b)$ If $A$ has finitely many prime ideals, prove that $A$ is PID. Does the converse hold?
   $(c)$ Show that, for any ideal $I \lhd A$, any ideal in $A/I$ is principal. Deduce that every ideal of $A$ is generated by two elements.

9. (5 points) Let $A$ be an integral domain with $\dim A \geq 1$. Show that $A$ is Dedekind if and only if there is a unique factorization of ideals as a product of prime ideals.

10. (5 points) Show that Dedekind domian is hereditary, in other words, each ideal is a projective module.

    **Remark.** For an integral domain $A$, it is Dedekind if and only if it is hereditary.

11. (3+3 points) Let $f(x, y) \in \mathbb{C}[x, y]$ be a nonsingular polynomial (ie. $(f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}) = (1)$ as ideals in $\mathbb{C}[x, y]$). Verify that $\mathbb{C}[x, y]/(f(x, y))$ is a Dedekind domain. What is the class group of $\mathbb{C}[x, y]/(f(x, y))$ if we further assume that $f$ is of the form $f(x, y) = y^2 - x^3 - ax - b$ where $x^3 + ax + b$ has no repeated roots (ie. $f$ is the equation of an elliptic curve)? (Compare to Problem 6 where the curve is *singular*.)