Math 538: Problem Set 2 (due 25/1/2017)

Number fields and rings of integers

Let $\mathbb{Q} \subset K \subset L$ be number fields with rings of integers $\mathcal{O}_K, \mathcal{O}_L$ respectively.

1. (Integers and Units) Let $\alpha \in \mathcal{O}_L$.
   (a) Show that $\mathrm{Tr}_K^L \alpha, N_K^L \alpha \in \mathcal{O}_K$.
   (b) Show that $\alpha \in \mathcal{O}_L^\times$ is a unit iff $N_K^L \varepsilon \in \mathcal{O}_K^\times$.

2. (Ideals)
   (a) Let $\alpha \in \mathcal{O}_L$. Show that $N_K^L \alpha \in \alpha\mathcal{O}_L$.
   (b) Conclude that any non-zero ideal $\mathfrak{a} \lhd \mathcal{O}_L$ contains an ideal of the form $m\mathcal{O}_L$, $m \in \mathbb{Z} \setminus \{0\}$.
   (c) Show that every non-zero ideal of $\mathcal{O}_L$ is a free Abelian group of rank $n = [L : \mathbb{Q}]$.

3. (Dedekind) Let $K = \mathbb{Q}(\theta)$ where θ is a root of $f(x) = x^3 - x^2 - 2x - 8$.
   (a) Show that f is irreducible over $\mathbb{Q}$.
   (b) Verify that $\eta = \frac{\theta^2+\theta}{2}$ satisfies $\eta^3 - 3\eta^2 - 10\eta - 8 = 0$.
   (c) Show that $1, \theta, \eta$ are linearly independent over $\mathbb{Q}$.
   (d) Let $M = \mathbb{Z} \oplus \mathbb{Z}\theta \oplus \mathbb{Z}\eta$ and let $N = \mathbb{Z}[\theta] = \mathbb{Z} \oplus \mathbb{Z}\theta \oplus \mathbb{Z}\theta^2$. Show that $N \subset M \subset \mathcal{O}_K$.
   (e) Calculate $D_{K/\mathbb{Q}}(M)$, $D_{K/\mathbb{Q}}(N)$ (hint: $D_{K/\mathbb{Q}}(N) = -4 \cdot 503$).
   (f) Show that $M = \mathcal{O}_K$
   (g) Let $\delta = A + B\theta + C\eta$ with $A, B, C \in \mathbb{Z}$. Show that $2 | d_{K/\mathbb{Q}}(\mathbb{Z}[\delta])$, and conclude that $\mathbb{Z}[\delta] \neq \mathcal{O}_K$.

   RMK Meditate on the conclusion of (g).

Generalization: Orders in $\mathbb{Q}$-algebras

DEFINITION. Let R be a commutative ring. An (associative, unital) *R-algebra* is a (possibly non-commutative) unital ring A equipped with a ring homomorphism $f \colon R \to A$ whose image is central. Equivalently, A is an R-module equipped with an associative, unital product which is R-bilinear.

DEFINITION. Let A be a $\mathbb{Q}$-algebra. A subring $\mathcal{O} \subset A$ is an *order* of A if it is the free $\mathbb{Z}$-module generated by a $\mathbb{Q}$-basis of A.

4. Fix a finite-dimensional $\mathbb{Q}$-algebra A.
   (a) Show that A contains orders.
   (b) Let $\mathcal{O} \subset A$ be an order. Show that every $x \in \mathcal{O}$ is integral over $\mathbb{Z}$.
   (c) Suppose that A is commutative. Show that A has a unique maximal order.

5. Define the *trace* of $x \in A$ as the trace of left multiplication by x. Given $\{x_i\}_{i=1}^n \subset A$ let $D(x_1, \ldots, x_n) \in M_n(\mathbb{Q})$ be the matrix with i, j entry $\mathrm{Tr}(x_i x_j)$, $\Delta(x_1, \ldots, x_n) = \det D(x_1, \ldots, x_n)$.
   (a) Let $\mathcal{O} \subset A$ be an order. Show that $\mathrm{Tr}\, x \in \mathbb{Z}$ for all $x \in \mathcal{O}$.
   (b) Let $\{\omega_i\}_{i=1}^n \subset A$ be a $\mathbb{Q}$-basis. Show that for any $\{x_i\}_{i=1}^n \subset A$, $\Delta(x_1, \ldots, x_n) = (\det\alpha)^2 \Delta(\omega_1, \ldots, \omega_n)$ where $\alpha \in M_n(\mathbb{Q})$ is the matrix such that $x_i = \sum_{k=1}^n \alpha_{ik}\omega_k$.

   COR Either $D = 0$ for all n-tuples (we say that the trace form is *degenerate*) or $D \neq 0$ for all bases (we say that the trace form is *non-degenerate*). We assume the second case from now on.

(c) Let $\mathcal{O}$ be an order with $\mathbb{Z}$-basis $\{\omega_i\}_{i=1}^n$. Show that the number $\Delta(\omega_1,\ldots,\omega_n)$ is a rational integer, independent of the choice of basis. Denote this $\Delta(\mathcal{O})$.

(d) Suppose that $\mathcal{O} \subset \mathcal{O}'$ are two orders. Show that $\Delta(\mathcal{O}) = [\mathcal{O}' : \mathcal{O}]^2 \Delta(\mathcal{O}')$ and deduce that in a non-degenerate $\mathbb{Q}$-algebra every order is contained in a maximal order.

(e) Construct a degenerate $\mathbb{Q}$-algebra without maximal orders.

REMARK. We have here a procedure for finding maximal orders in an n-dimensional $\mathbb{Q}$-algebras: start from a $\mathbb{Q}$-basis containing 1_A and scale its elements to obtain a Z-basis for an order $\mathcal{O}$, say of discriminant $\Delta(\mathcal{O})$. Let $\mathcal{O}'$ be an order containing $\mathcal{O}$ with index $d = [\mathcal{O}' : \mathcal{O}]$. Then $d\mathcal{O}' \subset \mathcal{O}$ so $\mathcal{O} \subset \mathcal{O}' \subset \frac{1}{d}\mathcal{O}$. Now $\frac{1}{d}\mathcal{O}/\mathcal{O} \simeq \left(\frac{1}{d}\mathbb{Z}/\mathbb{Z}\right)^n \simeq (\mathbb{Z}/d\mathbb{Z})^n$, so the set of $\mathbb{Z}$-submodules of $\frac{1}{d}\mathcal{O}$ containing $\mathcal{O}$ is finite and can be enumerated explicitely. It remains to check those one-by-one to see if any are orders; since $d^2 \mid \Delta(\mathcal{O})$ we only have finitely many values of d to check.

6. Now suppose that A is an F-algebra where F is a number field. Let $\mathcal{O} \subset A$ be an order. Show that the $\mathcal{O}_F$-submodule of A generated by $\mathcal{O}$ is an order as well.
   COR Every maximal order of A is an $\mathcal{O}_F$-module.
   RMK In fact, every order of A which is an $\mathcal{O}_F$-module is a *free* $\mathcal{O}_F$-module. We may discuss this later.