TD 2 : Anneaux d'entiers de corps de nombres

Exercice 1. [Rappels du TD précédent]

(*a*) Pour $\alpha \in \mathbb{C}$ algébrique et $K = \mathbb{Q}(\alpha)$, montrer que le polynôme minimal de α sur $\mathbb{Q}$ est exactement

$$P = \prod_{\sigma}(X - \sigma(\alpha))$$

où σ parcourt les plongements de K dans $\mathbb{C}$. En déduire la trace et la norme de α sur $\mathbb{Q}(\alpha)$.

(*b*) Montrer que pour $n \in \mathbb{N}^*$ et $C > 0$ fixés il n'existe qu'un nombre fini d'entiers algébriques α sur $\mathbb{C}$ de degré au plus n tels que $|\sigma(\alpha)| \leq C$ pour tout plongement σ de $\mathbb{Q}(\alpha)$ dans $\mathbb{C}$.

(*c*) Trouver $\alpha \in \mathbb{C}$ tel que $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = \pm 1$ mais α n'est pas un entier algébrique.

Exercice 2. [Anneaux de Dedekind]

(*a*) En trouvant un élément de $\mathbb{Q}[\sqrt{-3}]$ entier sur l'anneau $\mathbb{Z}[\sqrt{-3}]$, démontrer que ce dernier n'est pas de Dedekind.

(*b*) Donner deux exemples (pas trop similaires ni triviaux !) d'anneaux de Dedekind qui ne sont pas des anneaux d'entiers de corps de nombres.

(*c*) Montrer qu'un anneau de Dedekind est factoriel si et seulement si il est principal.

(*d*) (*Plus difficile)* Montrer que les idéaux d'un anneau de Dedekind sont tous engendrés par deux éléments.

Exercice 3. [Anneaux d'entiers relatifs]

Soient A, B deux anneaux intègres commutatifs unitaires, avec $A \subset B$. On dit que $b \in B$ est entier sur A s'il est annulé par un $P \in A[X]$ non nul.

(*a*) Montrer que $b \in B$ est entier sur A si et seulement si la multiplication par B stabilise un certain A-module de type fini inclus dans B.

(*b*) En déduire que l'ensemble des éléments de B entiers sur A est un anneau.

(*c*) Si K est un corps de nombres, montrer que tout élément de K entier sur $\mathcal{O}_K$ est déja dans $\mathcal{O}_K$. En déduire que tout anneau $A \subset K$ qui est un $\mathbb{Z}$-module de type fini est inclus dans $\mathcal{O}_K$.

Exercice 4. [Un exemple d'anneau d'entiers non monogène]

Soit $K = \mathbb{Q}(\sqrt{7}, \sqrt{10})$ et $\alpha \in \mathcal{O}_K$ de polynôme minimal P sur $\mathbb{Q}$. Pour tout polynôme Q de $\mathbb{Z}[X]$, on notera $\overline{Q}$ sa réduction dans $\mathbb{F}_3[X]$.

(*a*) Montrer que 3 divise $Q(\alpha)$ dans $\mathbb{Z}[\alpha]$ si et seulement si $\overline{P}$ divise $\overline{Q}$ dans $\mathbb{F}_3[X]$.

On suppose désormais que $\mathbb{Z}[\alpha] = \mathcal{O}_K$.

(*b*) Soient les entiers algébriques $\alpha_1 = (1+\sqrt{7})(1+\sqrt{10})$, $\alpha_2 = (1+\sqrt{7})(1-\sqrt{10})$, $\alpha_3 = (1-\sqrt{7})(1+\sqrt{10})$ et $\alpha_4 = (1-\sqrt{7})(1-\sqrt{10})$. Montrer que tous les $\alpha_i\alpha_j$ $(i \neq j)$ sont divisibles par 3 dans $\mathbb{Z}[\alpha]$, mais qu'aucune des puissances α_i^n ne l'est en considérant leur trace.

(*c*) Soient $P_i \in \mathbb{Z}[X]$, $1 \leq 4$ des polynômes tels que $P_i(\alpha) = \alpha_i$. Montrer que $\overline{P}$ divise les $\overline{P_iP_j}$ $(i \neq j)$ mais aucune des puissances $\overline{P_i}^n$. En déduire que pour tout i entre 1 et 4, $\overline{P}$ possède un facteur irréductible divisant $\overline{P_j}$ pour $j \neq i$ mais pas $\overline{P_i}$.

(*d*) En déduire que $\overline{P}$ a quatre facteurs irréductibles distincts, puis une contradiction. Ceci prouve que l'anneau $\mathcal{O}_K$ n'est pas de la forme $\mathbb{Z}[\alpha]$.

Exercice 5. [Décomposition des nombres premiers dans $\mathcal{O}_K$]

Soit K un corps de nombres, $\alpha \in \mathcal{O}_K$ tel que $\mathcal{O}_K = \mathbb{Z}[\alpha]$ et p un nombre premier de $\mathcal{O}_K$.

(*a*) Si P est le polynôme minimal de α sur $\mathbb{Q}$ et $\overline{P} = \prod_{i=1}^{r} \overline{P_{ii}}^{e}$ sa décomposition en facteurs irréductibles modulo p, montrer que quels que soient les choix de relèvement $P_i \in \mathbb{Z}[X]$ des $\overline{P_i}$, les idéaux premiers de $\mathcal{O}_K$ contenant p sont exactement les idéaux (distincts) $(p, P_i(\alpha))$.

(*b*) Montrer que $p\mathcal{O}_K = \prod_{i=1}^{r}(p, P_i(\alpha))_i^e$.

(*c*) Pour $d \in \mathbb{Z}$ sans facteur carré et différent de 0 et 1, donner pour tout nombre premier p un critère déterminant la forme de la décomposition de $p\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ en idéaux premiers.

*