TD10 : Finitude en algèbre commutative

Diego Izquierdo

Les exercices 0, 0', 1, 2 et 7 ont été traités en TD.

Exercice 0 (à préparer) : Exercices de théorie de Galois
Faire l'exercice 15 du TD8 et l'exercice 10 du TD9.

Exercice 0' : Et un dernier exercice de théorie de Galois
Faire l'exercice 14 du TD9.

Exercice 1 (à préparer) : Vrai ou faux ?

1. La $\mathbb{C}$-algèbre $\mathbb{C}[T,T^{-1}]$ est de type fini et il existe $a \in \mathbb{C}[T,T^{-1}]$ tel que $\mathbb{C}[T,T^{-1}]$ est une $\mathbb{C}[a]$ algèbre finie.
2. Si α est un nombre algébrique, alors $\mathbb{Z}[\alpha]$ est une $\mathbb{Z}$-algèbre de type fini qui n'est pas forcément finie.
3. Si α est un entier algébrique, alors $\mathbb{Z}[\alpha]$ est une $\mathbb{Z}$-algèbre finie.
4. L'anneau intègre $\mathbb{Q}[X,Y]/(X^3-Y^5)$ est intégralement clos.
5. Le nombre $\frac{1+\sqrt[3]{3}+3\sqrt[3]{3}}{2}$ est un entier algébrique.
6. Soit p un nombre premier. L'ensemble des polynômes $Q \in \mathbb{F}_p[X_1,...,X_p]$ tels que $Q(X_1,...,X_p) = Q(X_2+1, X_3+1, ..., X_p+1, X_1+1)$ est une $\mathbb{F}_p$-algèbre de type fini.
7. Soit A un anneau principal. Soit B une A-algèbre de type fini. Il existe alors des éléments $a_1,...,a_d \in B$ algébriquement indépendants sur A tels que $A[a_1,...,a_d] \subseteq B$ est une extension finie d'anneaux.

Exercice 2 (à préparer) : Anneau des entiers d'une extension quadratique de $\mathbb{Q}$
Soit d un entier différent de 0 et 1 et sans facteurs carrés. Soit $K = \mathbb{Q}(\sqrt{d})$. On cherche à déterminer l'anneau des entiers $\mathcal{O}_K$.

1. Montrer qu'un élément de K est un entier algébrique si, et seulement si, $N_{K/\mathbb{Q}}(x)$ et $\mathrm{Tr}_{K/\mathbb{Q}}(x)$ sont dans $\mathbb{Z}$.
2. En déduire que $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ si $d \not\equiv 1 \mod 4$ et que $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ si $d \equiv 1 \mod 4$.

Exercice 3 : Extensions biquadratiques
Soient $m, n \in \mathbb{Z} \setminus \{0,1\}$ distincts sans facteurs carrés. Soit $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$.

1. Calculer l'anneau des entiers $\mathcal{O}_K$ de K en fonction de m et n. En particulier, montrer que $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}\right]$ si $m \equiv n \equiv 1 \mod 4$.
2. Dans le cas $m \equiv n \equiv 1 \mod 8$, montrer qu'il n'existe pas d'élément $x \in \mathcal{O}_K$ tel que $\mathcal{O}_K = \mathbb{Z}[x]$. On pourra déterminer le cardinal de l'ensemble des morphismes d'anneaux de $\mathcal{O}_K$ à valeurs dans $\mathbb{Z}/2\mathbb{Z}$.

Exercice 4 : Anneaux d'entiers d'extensions cubiques 1

1. Montrer que l'anneau des entiers de $\mathbb{Q}(\sqrt[3]{2})$ est $\mathbb{Z}[\sqrt[3]{2}]$.

> **Indications :** Soit $\mathcal{O}$ l'anneau des entiers de $K = \mathbb{Q}(\sqrt[3]{2})$. Soit $x = a + b\sqrt[3]{2} + c\sqrt[3]{4} \in \mathcal{O}$ avec $a, b, c \in \mathbb{Q}$. On a :
>
> $$Tr_{K/\mathbb{Q}}(x) = 3a \in \mathbb{Z}, \quad Tr_{K/\mathbb{Q}}(x\sqrt[3]{2}) = 6c \in \mathbb{Z}, \quad Tr_{K/\mathbb{Q}}(x\sqrt[3]{2}) = 6b \in \mathbb{Z}.$$
>
> On écrit donc $a = n/3$, $b = m/6$, $c = l/6$, avec n, m, l entiers. Le polynôme caractéristique de la multiplication par x sur le $\mathbb{Q}$-espace vectoriel K est :
>
> $$-X^3 + 3aX^2 + (6bc - 3a^2)X + a^3 + 2b^3 + 4c^3 - 6abc.$$
>
> De même, le polynôme caractéristique de la multiplication par $x\sqrt[3]{2}$ sur le $\mathbb{Q}$-espace vectoriel K est :
>
> $$-X^3 + 6cX^2 + (6ab - 12c^2)X + 8c^3 + 2a^3 + 4b^3 - 12abc.$$
>
> On en déduit que $6bc - 3a^2 \in \mathbb{Z}$, $a^3 + b^3 + c^3 - 6abc \in \mathbb{Z}$ et $6ab - 12c^2 \in \mathbb{Z}$. Autrement dit, $ml - 2n^2 \in 6\mathbb{Z}$ et $8n^3 + 2m^3 + 4l^3 - 12nml \in 216\mathbb{Z}$. On vérifie aisément que cela impose que 3 divise n, que 6 divise m et que 6 divise l. Par conséquent, $x \in \mathbb{Z}[\sqrt[3]{2}]$ et $\mathcal{O} = \mathbb{Z}[\sqrt[3]{2}]$.

2. Soit $\theta \in \mathbb{C}$ tel que $\theta^3 - \theta - 4 = 0$. Montrer que $(1, \theta, \frac{\theta+\theta^2}{2})$ est une $\mathbb{Z}$-base de l'anneau des entiers de $\mathbb{Q}(\theta)$.

> **Indications :** Soit $\mathcal{O}$ l'anneau des entiers de $K = \mathbb{Q}(\theta)$. Le discriminant de la base $(1, \theta, \theta^2)$ est :
>
> $$\Delta = -4 \cdot (-1)^3 - 27 \cdot (-1)^2 = 4 \cdot 107.$$
>
> Soit Δ_K le discriminant d'une base de $\mathcal{O}$. Comme $\mathcal{O}$ contient $\mathbb{Z}[\theta]$, on a : $\frac{\Delta}{\Delta_K} = [\mathcal{O} : \mathbb{Z}[\theta]]^2$. Donc $[\mathcal{O} : \mathbb{Z}[\theta]] \in \{1, 2\}$. Comme $\frac{\theta+\theta^2}{2}$ est racine de $X^3 - X^2 - 3X - 2$, on a $\frac{\theta+\theta^2}{2} \in \mathcal{O}$, et donc $(1, \theta, \frac{\theta+\theta^2}{2})$ est une $\mathbb{Z}$-base de $\mathcal{O}$.

Exercice 5 : Anneaux d'entiers et polynômes d'Eisenstein

Soit $K/\mathbb{Q}$ une extension finie de degré n, soit $u \in \mathcal{O}_K$ tel que $K = \mathbb{Q}(u)$. Soit p un nombre premier tel que le polynôme minimal de u sur $\mathbb{Q}$ soit d'Eisenstein en p. L'objectif de l'exercice est de montrer que p ne divise pas l'indice de $\mathbb{Z}[u]$ dans $\mathcal{O}_K$.

1. Montrer que $\frac{u^n}{p} \in \mathcal{O}_K$ et que p^2 ne divise pas $N_{K/\mathbb{Q}}(u)$.

Indications : Soit $P = X^n + a_{n-1}X^{n-1} + ... + a_0$ le polynôme minimal de u. On a alors :

$$\frac{u^n}{p} = -\frac{a_{n-1}}{p}u^{n-1} - ... - \frac{a_0}{p} \in \mathcal{O}_K.$$

De plus, on a $|N_{K/\mathbb{Q}}(u)| = |a_0|$, donc p^2 ne divise pas $N_{K/\mathbb{Q}}(u)$.

2. Supposons que $p|[\mathcal{O}_K : \mathbb{Z}[u]]$.

(a) Montrer qu'il existe $x \in \mathcal{O}_K \setminus \mathbb{Z}[u]$ tel que $px \in \mathbb{Z}[u]$. En déduire qu'il existe $b_0, ..., b_{n-1} \in \mathbb{Z}$ non tous divisibles par p tels que $x = \frac{b_0+...+b_{n-1}u^{n-1}}{p}$.

Indications : On remarque que $\mathcal{O}_K/\mathbb{Z}[u]$ est un groupe abélien fini d'ordre multiple de p. Il possède donc un élément d'ordre p. En le relevant à $\mathcal{O}_K$, on obtient $x \in \mathcal{O}_K \setminus \mathbb{Z}[u]$ tel que $px \in \mathbb{Z}[u]$. On en déduit immédiatement qu'il existe $b_0, ..., b_{n-1} \in \mathbb{Z}$ non tous divisibles par p tels que $x = \frac{b_0+...+b_{n-1}u^{n-1}}{p}$.

(b) Notons r le plus petit entier tel que b_r n'est pas divisible par p. Montrer que $y = \frac{b_r u^r+...+b_{n-1}u^{n-1}}{p}$ est dans $\mathcal{O}_K$.

Indications : Comme p divise $b_0, ..., b_{r-1}$, on a $\frac{b_0+b_1u+...+b_{r-1}u^{r-1}}{p} \in \mathcal{O}_K$. Donc $y = x - \frac{b_0+b_1u+...+b_{r-1}u^{r-1}}{p} \in \mathcal{O}_K$.

(c) Montrer que $z = \frac{b_r u^{n-1}}{p} \in \mathcal{O}_K$.

Indications : On a $u^{n-1-r}y = \frac{b_r u^{n-1}+b_{r+1}u^n+...+b_{n-1}u^{2n-r-2}}{p} \in \mathcal{O}_K$. Mais, la question 1 montre que $\frac{b_{r+1}u^n+...+b_{n-1}u^{2n-r-2}}{p} \in \mathcal{O}_K$. Donc $z = \frac{b_r u^{n-1}}{p} \in \mathcal{O}_K$.

(d) Obtenir une contradiction en calculant la norme de z.

Indications : Soit a_0 le coefficient constant du polynôme minimal de u. On a $N_{K/\mathbb{Q}}(z) = \frac{b_r^n N_{K/\mathbb{Q}}(u)^{n-1}}{p^n} \in \mathbb{Z}$. Cela est absurde car p ne divise pas b_r et p^2 ne divise pas $N_{K/\mathbb{Q}}(u)$.

3. Si q est une puissance de p et $K = \mathbb{Q}(\sqrt[q]{p})$, montrer que $\mathcal{O}_K = \mathbb{Z}[\sqrt[q]{p}]$.

Indications : Le discriminant de $X^q - p$ est $\pm q^q \cdot p^{q-1}$. Donc $[\mathcal{O}_K : \mathbb{Z}[\sqrt[q]{p}]]$ est une puissance de p. Mais, comme $X^q - p$ est Eisenstein, la question 2 montre que p ne divise pas $[\mathcal{O}_K : \mathbb{Z}[\sqrt[q]{p}]]$. Par conséquent, $\mathcal{O}_K = \mathbb{Z}[\sqrt[q]{p}]$.

Exercice 6 : Anneaux d'entiers d'extensions cubiques 2

Soit $d \in \mathbb{Z}$, $d > 1$ sans facteur cubique. Notons $\theta = \sqrt[3]{d}$ et $K = \mathbb{Q}(\theta)$. On cherche à déterminer l'anneau des entiers $\mathcal{O}_K$ de K.

1. Montrer que la base $(1, \theta, \theta^2)$ est de discriminant $\Delta = -27d^2$.

Indications : Le discriminant Δ est le discriminant du polynôme $X^3 - d$: c'est donc $-27d^2$.

2. On écrit $d = ab^2$, avec $a, b \in \mathbb{N}$ sans facteur carré. On pose $\theta' = \sqrt[3]{a^2 b}$. Montrer que $K = \mathbb{Q}(\theta')$ et calculer le discriminant Δ' de la base $(1, \theta', \theta'^2)$.

Indications : Les polynômes $X^3 - d$ et $X^3 - a^2b$ sont de degré 3. Donc $[K : \mathbb{Q}] = [\mathbb{Q}(\theta') : \mathbb{Q}] = 3$. De plus, $\theta\theta' = ab \in \mathbb{Q}$. Donc $K = \mathbb{Q}(\theta')$. Le discriminant de la base $(1, \theta', \theta'^2)$ est $\Delta' = -27a^4b^2$.

3. Montrer que $(1, \theta, \theta')$ est une $\mathbb{Q}$-base de K et calculer son discriminant Δ''.

Indications : On a $\theta' = \frac{ab}{\theta} = \frac{ab\theta^2}{d}$. Donc $(1, \theta, \theta')$ est une $\mathbb{Q}$-base de K et $\Delta'' = \left(\frac{ab}{d}\right)^2 \Delta = -27a^2b^2$.

4. On note f, f' et f'' les indices respectifs de $\mathbb{Z}[\theta]$, $\mathbb{Z}[\theta']$ et $\mathbb{Z} \oplus \mathbb{Z}\theta \oplus \mathbb{Z}\theta'$ dans $\mathcal{O}_K$.

(a) Montrer que toutes les $\mathbb{Z}$-bases de $\mathcal{O}_K$ ont même discriminant. On le note Δ_K.

Indications : Soient B et B' deux bases de $\mathcal{O}_K$, de discriminants Δ_B et $\Delta_{B'}$. Il existe alors $P \in GL_3(\mathbb{Z})$ telle que $B = PB'$. On a alors $\Delta_B = (\det P)^2 \Delta_{B'} = \Delta_{B'}$.

(b) Montrer que $f^2 = \frac{\Delta}{\Delta_K}$, $f'^2 = \frac{\Delta'}{\Delta_K}$ et $f''^2 = \frac{\Delta''}{\Delta_K}$.

Indications : Soit B_0 une base de $\mathcal{O}_K$ et $B = (1, \theta, \theta^2)$. Soit $P \in M_n(\mathbb{Z})$ telle que $PB_0 = B$. On a alors :

$$\Delta = (\det P)^2 \Delta_K = f^2 \Delta_K.$$

Les autres égalités sont analogues.

(c) Montrer que $a \wedge f = 1$ et que $b \wedge f' = 1$. On pourra utiliser l'exercice 5.

Indications : Si p est un nombre premier divisant a, on remarque que $X^3 - d$ est p-Eisenstein, donc $a \wedge f = 1$. De même, si p est un nombre premier divisant b, on remarque que $X^3 - a^2b$ est p-Eisenstein, donc $b \wedge f' = 1$.

(d) En déduire les assertions suivantes :

(i) $\Delta_K < 0$;

Indications : $\Delta_K = f^{-2}\Delta = -27d^2f^{-2} < 0$.

(ii) $a^2b^2 | \Delta_K | 27a^2b^2$;

Indications : On a : $\Delta_K | \Delta'' = -27a^2b^2$. Par ailleurs, $a \wedge f = 1$ et $\Delta_K = \frac{-27a^2b^4}{f^2}$, donc $a^2 | \Delta_K$. De même, $b^2 | \Delta_K$. Donc $a^2b^2 | \Delta_K$.

(iii) si $3|a$, alors $27a^2 | \Delta_K$;

Indications : Cela découle du fait que $a \wedge f = 1$ et que $\Delta_K = \frac{-27a^2b^4}{f^2}$.

(iv) si $3|b$, alors $27b^2 | \Delta_K$.

Indications : Analogue à (iii).

5. Montrer que si $3|d$, alors $\Delta_K = -27a^2b^2$ et $(1, \theta, \theta')$ est une base de $\mathcal{O}_K$.

Indications : Dans ce cas, 3 divise a ou b. Donc d'après 4(d), ou bien $27a^2$ et b^2 divisent Δ_K, ou bien $27b^2$ et a^2 divisent Δ_K. Dans les deux cas, $27a^2b^2 | \Delta_K$, et donc $\Delta_K = -27a^2b^2$. Donc $f'' = 1$, et $(1, \theta, \theta')$ est une base de $\mathcal{O}_K$.

6. Supposons que 3 ne divise pas d et que $d \pm 1$ n'est pas multiple de

9. Montrer que le polynôme minimal de $\theta - d$ est 3-Eisenstein. En procédant comme dans les questions précédentes, en déduire que $\Delta_K = -27a^2b^2$ et $(1, \theta, \theta')$ est une base de $\mathcal{O}_K$.

> **Indications :** Le polynôme minimal de $\theta - d$ est $(X+d)^3 - d$: il est donc 3-Eisenstein. Par conséquent, 3 ne divise pas f. De plus, $\Delta_K = \frac{-27a^2b^4}{f}$ et $a \wedge f = 1$. Donc $27a^2$ divise Δ_K. On peut montrer de même que $27b^2$ divise Δ_K. Donc $27a^2b^2$ divise Δ_K, et $\Delta_K = -27a^2b^2$. On conclut ensuite comme dans la question 5.

7. On suppose $d \equiv 1 \mod 9$. On pose $\alpha = \frac{1+\theta+\theta^2}{3}$.

(i) Montrer que $\alpha \in \mathcal{O}_K$ et calculer son polynôme minimal.

> **Indications :** Le polynôme minimal de α est $X^3 - X^2 - \frac{d-1}{3}X - \frac{(d-1)^2}{27}$. Il est à coefficients dans $\mathbb{Z}$. Donc $\alpha \in \mathcal{O}_K$.

(ii) En déduire que $3|f''$, puis que $\Delta_K = -3a^2b^2$.

> **Indications :** Dans le quotient $\mathcal{O}_K/(\mathbb{Z} \oplus \mathbb{Z}\theta \oplus \mathbb{Z}\theta')$, on remarque que $ab\alpha$ est non trivial et que $3ab\alpha$ est trivial. Donc $\mathcal{O}_K/(\mathbb{Z} \oplus \mathbb{Z}\theta \oplus \mathbb{Z}\theta')$ possède un élément d'ordre 3, et 3 divise f''. Donc $\Delta_K | 3a^2b^2$. Mais en plus, $\frac{-27a^2b^2}{\Delta_K}$ est un carré et $a^2b^2 | \Delta_K$. Donc $\Delta_K = 3a^2b^3$.

(iii) Montrer que $(\alpha, \theta, \theta')$ est une $\mathbb{Z}$-base de $\mathcal{O}_K$.

> **Indications :** Le discriminant de $(\alpha, \theta, \theta')$ est $-3a^2b^2$. Donc $(\alpha, \theta, \theta')$ est une $\mathbb{Z}$-base de $\mathcal{O}_K$.

8. Supposons $d \equiv -1 \mod 9$. On pose $\alpha' = \frac{1-\theta+\theta^2}{3}$. Montrer que $(\alpha', \theta, \theta')$ est une $\mathbb{Z}$-base de $\mathcal{O}_K$.

> **Indications :** Analogue à la question 7.

Exercice 7 : Anneaux d'entiers de corps cyclotomiques 1

Soient p un nombre premier et $k \geq 1$ un entier. Soient $\overline{\mathbb{Q}}$ une clôture algébrique fixée de $\mathbb{Q}$ et $\zeta \in \overline{\mathbb{Q}}$ une racine primitive p^k-ème de l'unité. Soit $\mathcal{O}_{p^k}$ l'anneau des entiers algébriques de $\mathbb{Q}(\zeta)$.

1. Montrer l'identité $p = \prod_{\substack{r=1 \\ p \nmid r}}^{p^k} (1 - \zeta^r)$.

2. En déduire que $(\zeta - 1)\mathcal{O}_{p^k} \cap \mathbb{Z} = p\mathbb{Z}$.

Supposons $k = 1$.

3. En utilisant la trace, montrer que l'anneau $\mathcal{O}_p$ est égal à $\mathbb{Z}[\zeta]$.

Revenons au cas général $k \geq 1$.

4. Montrer que l'on a $\mathcal{O}_{p^k} = \mathbb{Z}[\zeta] + p^m\mathcal{O}_{p^k}$ pour tout $m \geq 0$.

5. Montrer que le discriminant de Φ_{p^k} est, au signe près, une puissance de p (que l'on explicitera).

6. En déduire que l'anneau $\mathcal{O}_{p^k}$ est égal à $\mathbb{Z}[\zeta]$.

Exercice 8 : Anneaux d'entiers de corps cyclotomiques 2

Soient K et L deux extensions galoisiennes finies de $\mathbb{Q}$ telles que $K \cap L = \mathbb{Q}$.

1. Montrer que l'extension composée KL de $\mathbb{Q}$ est galoisienne finie.

> **Indications :** Si K et L décomposent respectivement $P, Q \in \mathbb{Q}[X]$, alors $\mathbb{Q} \subseteq KL$ décompose PQ et est galoisienne finie.

2. Montrer que la restriction induit un isomorphisme de groupes $\mathrm{Gal}(KL/L) \cong \mathrm{Gal}(K/\mathbb{Q})$.

> **Indications :** Considérons le morphisme de restriction $\mathrm{Gal}(KL/L) \to \mathrm{Gal}(K/K \cap L)$: il est injectif puisque KL contient K. De plus, tout automorphisme de $\mathrm{Gal}(K/\mathbb{Q})$ peut s'étendre en un automophisme de KL par L-linéarité, ce qui est permis car on a $L \cap K = \mathbb{Q}$.

3. Montrer que l'application canonique $\mathrm{Gal}(KL/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$ est un isomorphisme de groupes.

> **Indications :** Soit $\varphi : \mathrm{Gal}(KL/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$ le morphisme de restriction. Il est injectif par définition de KL et surjectif en prolongeant successivement à L et à KL par 2.

Soit $\mathcal{O}_K$ (resp. $\mathcal{O}_L$, resp. $\mathcal{O}_{KL}$) l'anneau des entiers de K (resp. L, resp. KL). On note Δ_K (resp. Δ_L, resp. Δ_{KL}) le discriminant de K (resp. de L, resp. de KL), c'est-à-dire le discriminant d'une $\mathbb{Z}$-base de $\mathcal{O}_K$ (resp. $\mathcal{O}_L$, resp. $\mathcal{O}_{KL}$).

4. Expliquer pourquoi Δ_K et Δ_L sont bien définis et sont dans $\mathbb{Z}$.

> **Indications :** Soient B et B' deux bases de $\mathcal{O}_K$, de discriminants Δ_B et $\Delta_{B'}$. Il existe alors $P \in GL_3(\mathbb{Z})$ telle que $B = PB'$. On a alors $\Delta_B = (\det P)^2 \Delta_{B'} = \Delta_{B'}$. Donc Δ_K est bien défini.
> De plus, par définition du discriminant, $\Delta_K \in \mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$.

On suppose que Δ_K et Δ_L sont premiers entre eux. Soient $(a_1, \ldots, a_r)$ (resp. $(b_1, \ldots, b_s)$) une base du $\mathbb{Z}$-module $\mathcal{O}_K$ (resp. $\mathcal{O}_L$).
Soit $x = \sum_{i,j} x_{ij} a_i b_j \in \mathcal{O}_{KL}$ avec $x_{ij} \in \mathbb{Q}$. Pour $1 \leq i \leq r$, on note $x_i = \sum_j x_{ij} b_j$.

5. Montrer, pour tous i, j, que l'on a $\Delta_K x_i \in \mathcal{O}_L$, et donc $\Delta_K x_{ij} \in \mathbb{Z}$.

> **Indications :** Pour $g \in \mathrm{Gal}(KL/L)$, on écrit $g(x) = \sum_{i,j} x_{ij} g(a_i) b_j = \sum_i g(a_i) x_i$. En faisant varier $g \in \mathrm{Gal}(KL/L)$, on obtient
>
> $$\begin{pmatrix} g_1(x) \\ \vdots \\ g_r(x) \end{pmatrix} = \begin{pmatrix} g_1(a_1) & \ldots & g_1(a_r) \\ \vdots & & \vdots \\ g_r(a_1) & \ldots & g_r(a_r) \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix}.$$
>
> En particulier, les $g_1(x), \ldots, g_r(x)$ engendrent un sous-$\mathcal{O}_K$-module de celui engendré par les $x_1, \ldots, x_r$; et, par la question (b), il est d'indice divisant $\Delta_K = \left(\det\left((g_i(a_j))_{ij}\right)\right)^2 \in \mathbb{Z}$. De ce fait, pour tout i, $\Delta_K x_i$ appartient à $\sum_j \mathcal{O}_K g_j(x) \cap L \subseteq \mathcal{O}_{KL} \cap L = \mathcal{O}_L$. Par définition des b_j, on en déduit $\Delta_K x_{ij} \in \mathbb{Z}$ pour tous i, j.

6. En déduire que $\mathcal{O}_{KL} = \bigoplus_{\substack{1 \leq i \leq r \\ 1 \leq j \leq s}} a_i b_j \mathbb{Z}$ et que $\Delta_{KL} = \Delta_K^{[L:\mathbb{Q}]} \Delta_L^{[K:\mathbb{Q}]}$.

Indications : De la même manière, $\Delta_L x_{ij}$ est un entier relatif pour tous i, j. Parce que Δ_K et Δ_L, une utilisation du lemme de Bézout donne $x_{ij} \in \mathbb{Z}$ comme voulu. Maintenant que l'on dispose d'une $\mathbb{Z}$-base de $\mathcal{O}_{KL}$, il suffit de calculer pour obtenir la relation $\Delta_{KL} = \Delta_K^{[L:\mathbb{Q}]} \Delta_L^{[K:\mathbb{Q}]}$.

Soient $m, n \geq 1$ deux entiers premiers entre eux. Soient $\alpha, \beta \in \overline{\mathbb{Q}}$ des racines primitives respectivement m-ème et n-ème de l'unité.

7. Montrer $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$.

Indications : Comme m et n sont premiers entre eux, $\mathbb{Q}(\alpha, \beta)$ est le sous-corps de $\overline{\mathbb{Q}}$ engendré par une racine primitive mn-ème de l'unité : il est de degré $\varphi(mn)$ sur $\mathbb{Q}$ et de groupe de Galois $(\mathbb{Z}/mn\mathbb{Z})^\times \simeq (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. De plus, $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta)$ est fixe par le sous-groupe de $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ engendré par un générateur de $(\mathbb{Z}/m\mathbb{Z})^\times$ et un générateur de $(\mathbb{Z}/n\mathbb{Z})^\times$: il est fixe par tout $\mathrm{Gal}(\mathbb{Q}(\alpha, \beta)/\mathbb{Q})$ et on a $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$.

8. En utilisant l'exercice précédent, en déduire que l'anneau des entiers de $\mathbb{Q}(\alpha)$ est $\mathbb{Z}[\alpha]$.

Indications : On montre par récurrence sur le nombre de facteurs premiers de m la propriété suivante : l'anneau des entiers de $\mathbb{Q}(\alpha)$ est $\mathbb{Z}[\alpha]$ et les facteurs premiers du discriminant de $\mathbb{Q}(\alpha)$ sont contenus dans les facteurs premiers de m. L'initialisation se fait à l'aide de l'exercice 7, et l'hérédité utilise les questions 6 et 7.

Exercice 9 : Anneaux intégralement clos et polynômes

Soit A un anneau intégralement clos de corps des fractions K.

1. Soit $P \in A[X]$ tel que $P = QR$, avec $Q, R \in K[X]$ unitaires. Montrer que $Q, R \in A[X]$.

2. Montrer que $A[X]$ est intégralement clos.

Indications : Voir le théorème 8.23 du polycopié d'Algèbre 2 d'Olivier Debarre (`http://www.math.ens.fr/~debarre/`).

Exercice 10 : Extensions quadratiques, le retour

Soit A un anneau factoriel dans lequel 2 est inversible. Soit $a \in A$ qui n'est divisible par le carré d'aucun élément irréductible de A et qui n'est pas un carré. Montrer que $B = A[X]/(X^2 - a)$ est intégralement clos. Est-il forcément factoriel ?

Indications : Soit K le corps des fractions de A et $L = K(\sqrt{a})$ le corps des fractions de B. Soit $x = y + z\sqrt{a} \in L$ entier sur A. On a alors $Tr_{L/K}(x) = 2y \in A$ et $N_{L/K}(x) = x^2 - az^2 \in A$. Donc $y \in A$ et $az^2 \in A$. Comme A est factoriel et a n'a pas de facteurs carrés, on déduit aussi que $z \in A$. Donc $x \in B$ et B est intégralement clos. En prenant $A = \mathbb{C}[T]$ et $a = T(T+1)(T+2)$, l'anneau $B = \mathbb{C}[T, X]/(X^2 - T(T+1)(T+2))$ n'est pas factoriel.

Exercice 11 : Anneaux normaux et actions de groupes

Soit A un anneau intègre sur lequel agit un groupe fini G. On note A^G l'anneau des invariants.

1. Montrer que l'action de G s'étend en une action sur le corps de fractions K de A.

> **Indications :** Il suffit de poser $g \cdot \frac{a}{b} = \frac{g \cdot a}{g \cdot b}$ pour $g \in G$, $a \in A$ et $b \in A \setminus \{0\}$.

2. Montrer que le corps des fractions de A^G est K^G.

> **Indications :** Le corps des fractions est évidemment contenu dans K^G. Réciproquement, soit $x \in K^G$. Soient $a, b \in A$ tels que $x = \frac{a}{b}$. Pour chaque $g \in G$, on a $b(g \cdot a) = a(g \cdot b)$. Soit $c = \prod_{g \in G \setminus \{1\}} (g \cdot b)$. Pour $g_0 \in G \setminus \{1\}$, on a :
>
> $$g_0 \cdot (ac) = b(g_0 \cdot a) \prod_{g \in G \setminus \{1, g_0\}} (g \cdot b) = a(g_0 \cdot b) \prod_{g \in G \setminus \{1, g_0\}} (g \cdot b) = ac,$$
>
> $$g_0 \cdot (bc) = (g_0 \cdot b) \prod_{g \in G \setminus \{g_0\}} (g \cdot b) = bc.$$
>
> Donc $x = \frac{ac}{bc}$ est dans le corps des fractions de A^G.

3. Montrer que, si A est intégralement clos, alors A^G l'est aussi.

> **Indications :** Si $x \in K^G$ est entier sur A^G, alors il est entier sur A. Comme A est intégralement clos, on déduit que $x \in A$. Par conséquent, $x \in A \cap K^G = A^G$, et A^G est intégralement clos.