TD n°5.

Tous les anneaux sont supposés commutatifs. Si A est un anneau et $\mathfrak{p}$ est un idéal premier, on note $A_{\mathfrak{p}}$ le localisé de $\mathfrak{p}$ par la partie multiplicative $A - \mathfrak{p}$.

Exercice 1. Soit A un anneau. Montrer que le morphisme $A \to \prod_{\mathfrak{m} \text{ idéal maximal de } A} A_{\mathfrak{m}}$ qui envoie a sur $(a/1)$ est injectif.

Solution. Si a est envoyé sur 0 dans $A_{\mathfrak{m}}$, si et seulement si il existe $m \notin \mathfrak{m}$ tel que $ma = 0$. Donc a est dans le noyau de $A \to \prod_{\mathfrak{m} \text{ idéal maximal de } A} A_{\mathfrak{m}}$ si et seulement si l'annulateur de a n'est contenu dans aucun idéal maximal. Or tout idéal propre est contenu dans un idéal maximal. On devrait donc avoir $\mathrm{Ann}(a) = A$, ce qui implique que $a = 0$.

Exercice 2. Montrer qu'un anneau A est réduit (c'est-à-dire $\sqrt{0} = 0$) si et seulement si $A_{\mathfrak{m}}$ est réduit pour tout idéal maximal $\mathfrak{m}$.

Solution. Supposons A réduit et soit $a/s \in A_{\mathfrak{m}}$ tel que $(a/s)^n = 0$. Alors il existe $t \notin \mathfrak{m}$ tel que $ta^n = 0$, et donc $(ta)^n = 0$. Mais comme A est réduit, $ta = 0$ donc $a/s = 0$, ce qui montre que $A_{\mathfrak{m}}$ est réduit.
Réciproquement, si tous les $A_{\mathfrak{m}}$ sont réduit, alors $\prod A_{\mathfrak{m}}$ est aussi réduit, et donc A aussi puisque c'est un sous anneau de $\prod A_{\mathfrak{m}}$ d'après l'exo précédent.

Exercice 3. a) Soit A un sous-anneau de $\mathbb{Q}$ (contenant $\mathbb{Z}$). Soit $S = \mathbb{Z} \cap A^{\times}$. Montrer que $A = S^{-1}\mathbb{Z}$.

b) Généraliser en remplaçant $\mathbb{Z}$ par un anneau principal.

c) Trouver un sous-anneau de $\mathbb{C}(X, Y)$ contenant $\mathbb{C}[X, Y]$ qui ne soit pas, en tant que $\mathbb{C}[X, Y]$-algèbre, un localisé de $\mathbb{C}[X, Y]$.

Solution. a) $S^{-1}\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$ et on a clairement $S^{-1}\mathbb{Z} \subset A$ (tous les éléments de S étant inversibles dans A).
Réciproquement soit $p/q \in A$ avec p et q premiers entre eux. Soient $u, v \in \mathbb{Z}$ tels que $up + vq = 1$, alors $1/q = v + u(p/q) \in A$ car $v, u \in A$. Donc $q \in S$ et $p/q \in S^{-1}A$.
b) Soit A un anneau principal de corps des fractions K et B un sous anneau de K. Notons $S = A \cap B^{\times}$. Alors $B = S^{-1}A$. La preuve est identique à celle pour $\mathbb{Z}$.
c) Soit $A = \mathbb{C}[X, Y]$ et $B = \mathbb{C}[X, Y][X/Y]$. Alors $B^{\times} = \mathbb{C}^{\times}$. En effet, on a un isomorphisme de $\mathbb{C}$-algèbres $\mathbb{C}[T_1, T_2] \to B$ envoyant T_1 sur Y et T_2 sur X/Y (pour la surjectivité X est l'image de T_1T_2, l'injectivité se vérifie facilement par le fait que les monomes soit envoyés sur des monomes de degrés tous distincts). Pour déterminé les inversibles de B, on est donc ramené au cas d'une algèbre de polynôme, ce qui figure dans le cours. Donc si $B = S^{-1}A$ en tant que A-algèbre (attention : remarquez que A et B sont isomorphes en tant qu'anneaux ou même en tant que $\mathbb{C}$-algèbre. Le fait qu'on cherche ici un isomorphisme de A-algèbre n'est donc pas anodin), alors $S \subset B^{\times} = \mathbb{C}^{\times} = A^{\times}$. Donc $S^{-1}A = A$ or B n'est pas isomorphe à A en tant que A-algèbre puisque $X/Y \notin A$.

Exercice 4. Soit A un anneau, S une partie multiplicative de A, et M un A-module. On note $S^{-1}M = (M \times S)/\sim$ où $(m, s) \sim (m', s')$ si et seulement si il existe $r \in S$ tel que $r(s'm - sm') = 0$. On note m/s l'image de (m, s) dans $S^{-1}M$.
On vérifie que l'addition $(m/s) + (m'/s') = (s'm + sm')/(ss')$ et la multiplication externe $(a/s)(m/s') = am/ss'$ définissent une structure de $S^{-1}A$-module sur $S^{-1}M$ (et donc à fortiori de A-module).

a) Vérifier qu'il existe un unique morphisme de A-modules $f : M \otimes_A S^{-1}A \to S^{-1}M$ envoyant $m \otimes a/s$ sur am/s.

b) Montrer que f est un isomorphisme.

c) Montrer que $S^{-1}A$ est un A-module plat.

Exercice 5. Montrer qu'un A-module M est plat si et seulement si $M_{\mathfrak{m}}$ est un $A_{\mathfrak{m}}$-module plat pour tout idéal premier $\mathfrak{m}$ de A.

Exercice 6 (Going-up de Cohen-Seidenberg)**.** Soit $A \xrightarrow{f} B$ un morphisme injectif d'anneaux commutatifs. On suppose que f fait de B une A-algèbre entière. Montrer successivement que :

a) Si B est intègre, alors A est un corps si et seulement si B est un corps.

b) Si $\mathfrak{q}$ est un idéal premier de B, alors $\mathfrak{q}$ est maximal si et seulement si $\mathfrak{q} \cap A$ est maximal dans A.

c) Pour tout idéal premier $\mathfrak{p}$ de A, il existe un idéal premier $\mathfrak{q}$ de B tel que $\mathfrak{p} = \mathfrak{q} \cap A$ (on pourra s'intéresser au morphisme $A_{\mathfrak{p}} \to B_{\mathfrak{p}}$ et considérer un idéal maximal de $B_{\mathfrak{p}}$).
Traduire en termes de l'application $\mathrm{Spec}(f) : \mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$.

d) Si $\mathfrak{q} \subset \mathfrak{q}'$ sont deux idéaux premiers de B, alors $\mathfrak{q} \cap A = \mathfrak{q}' \cap A$ implique $\mathfrak{q} = \mathfrak{q}'$.

Exercice 7. Montrer que $\mathbb{Z}$ est intégralement clos.

Solution. Soit p/q, avec p et q premiers entre eux, solution d'un polynôme unitaire $P = X^n + \sum_{k<n} a_k X^k$. Alors $0 = q^n P(p/q) = p^n + \sum_{k<n} a_k p^k q^{n-k}$. Tous les termes de la somme sauf éventuellement p^n sont divisibles par q, en les passant de l'autre côté de l'égalité, on en déduit que p^n est divisible par q. Or p et q sont premiers entre eux, donc q est inversible et $p/q \in \mathbb{Z}$ comme voulu.

Exercice 8. Soit $\mathbb{Q}[i]$ le sous-anneau de $\mathbb{C}$ engendré par $\mathbb{Q}$ et i.

a) Vérifier que $1, i$ forme une base de $\mathbb{Q}[i]$ en tant que $\mathbb{Q}$-espace vectoriel.

b) Montrer que $a + bi \in \mathbb{Q}[i]$, avec $a, b \in \mathbb{Q}$, est entier sur $\mathbb{Z}$ si et seulement si $a, b \in \mathbb{Z}$.

Solution. a) 1 et i forment une $\mathbb{Q}$-famille libre car ils forment même une $\mathbb{R}$-famille libre dans $\mathbb{C}$. De plus $\mathbb{Q}[i]$ est engendré par $(i^n, n \in \mathbb{N})$ en tant que $\mathbb{Q}$-ev, et $i^n = 1, -1, i$ ou $-i$ pour tout n, donc est bien dans l'espace engendré par 1 et i. Donc $(1, i)$ est une famille génératrice.

b) Si $P(a + ib) = 0$ avec P unitaire dans $\mathbb{Z}[X]$, alors $P(a - ib) = \overline{P(a + ib)} = 0$, donc $a - ib$ est aussi entier sur $\mathbb{Z}$. Comme les entiers forment un anneau? on en déduit que $a^2 + b^2 = (a + ib)(a - ib)$ et $2a = (a + ib) + (a - ib)$ sont aussi entiers sur $\mathbb{Z}$. Or $a^2 + b^2, 2a \in \mathbb{Q}$, donc comme $\mathbb{Z}$ est intégralement clos d'après la question précédente, on a $a^2 + b^2, 2a \in \mathbb{Z}$.
Donc $(2a)^2 + 4b^2 \in 4\mathbb{Z} \subset \mathbb{Z}$ et donc $(2b)^2 = 4b^2 \in \mathbb{Z}$. Comme $\mathbb{Z}$ est intégralement clos, $2b \in \mathbb{Z}$. En posant $a' = 2a$ et $b' = 2b$, on obtient que $(a')^2 + (b')^2$ doit être multiple de 4. En regardant les différentes possibilités pour a' et b' mod 2, on trouve que a' et b' doivent être pairs, et donc a, b sont entiers.
Réciproquement i est entier sur $\mathbb{Z}$ car $X^2 + 1$ en est un polynome annulateur. Comme les entiers forment un anneau, $a + bi$ est aussi entier sur $\mathbb{Z}$ pour tout $a, b \in \mathbb{Z}$.

Exercice 9. Soit $d \in \mathbb{Z}$ un entier non inversible sans facteur carré ($a^2 | d$ implique a inversible). On note $K := \mathbb{Q}[\sqrt{d}]$ la sous-algèbre de $\mathbb{C}$ engendré par $\mathbb{Q}$ et $\sqrt{d}$ (où $\sqrt{d}$ est un élément de $\mathbb{C}$ tel que $\sqrt{d}^2 = d$ choisi arbitrairement).

a) Montrer que $(1, \sqrt{d})$ est une base de K en tant que $\mathbb{Q}$-espace vectoriel. En déduire que K est un corps.

b) Montrer que $s : K \to K$ qui à $a + b\sqrt{d}$ associé $a - b\sqrt{d}$ est un automorphisme de corps.

c) Montrer que $x \in K$ est entier sur $\mathbb{Z}$ si et seulement si $N(x) := xs(x) \in \mathbb{Z}$ et $T(x) := x + s(x)$ sont dans $\mathbb{Z}$.

d) On suppose $d = -3$. Donner une base du $\mathbb{Z}$-module O_K.

Solution. a) $\sqrt{d}^{2n} = d^n \in 1\mathbb{Q}$ et $\sqrt{d}^{2n+1} = d^n \sqrt{d} \in \sqrt{d}\mathbb{Q}$, donc $1, \sqrt{d}$ engendre $\sum_n \sqrt{d}^n \mathbb{Q} = \mathbb{Q}[\sqrt{d}]$. De plus $1, \sqrt{d}$ forment une famille $\mathbb{Q}$-libre car $\sqrt{d} \notin \mathbb{Q}$.
K est un sous-anneau de $\mathbb{C}$, il est donc intègre. De plus c'est un $\mathbb{Q}$-algèbre intègre de dimension fini en tant que $\mathbb{Q}$-espace vectoriel, c'est donc un corps.

b) s est clairement $\mathbb{Q}$-linéarie et on vérifie à la main $s(xy) = s(x)s(y)$.

c) Si x est entier sur $\mathbb{Z}$, soit $P \in \mathbb{Z}[X]$ unitaire annulant x. Alors $P(s(x)) = s(P(x)) = 0$ (car les coefficients de P sont fixes par s), donc $s(x)$ est également entier sur $\mathbb{Z}$, donc $N(x)$ et $T(x)$ sont aussi entiers sur $\mathbb{Z}$ (les entiers forment un anneau). Or $N(a + b\sqrt{d}) = a^2 - db^2, T(a + b\sqrt{d}) = 2a \in \mathbb{Q}$ et comme $\mathbb{Z}$ est intégralement clos, on obtient donc $N(x), T(x) \in \mathbb{Z}$.
Réciproquement, si $N(x), T(x) \in \mathbb{Z}$, alors $X^2 - T(x)X + N(x) = (X - x)(X - s(x))$ est un polynôme de $\mathbb{Z}[X]$ unitaire annulant x, donc x est entier sur $\mathbb{Z}$.

d) On doit résoudre $a^2 + 3b^2 \in \mathbb{Z}, 2a \in \mathbb{Z}$ pour $a, b \in \mathbb{Q}$.
En posant $a' = 2a, b' = 2b$, on obtient $a' \in \mathbb{Z}$ et $a'^2 + 3b'^2 \in 4\mathbb{Z}$. La deuxième équation nous donne $3b'^2 \in \mathbb{Z}$ ce qui n'est possible que si $b' \in \mathbb{Z}$. En regardant les valeurs possible modulo 2 pour a' et b', on obtient que $a'^2 + 3b'^2 \in 4\mathbb{Z}$ si et seulement si a et b' sont de même parité. Il en découle que $O_K = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{-3}}{2}$