Feuille TD 2 – Exercices Algèbre – Anneaux

Exercice 1. Montrer que tout anneau intègre fini est un corps.

Exercice 2. Soit A un anneau commutatif, et soit S une partie multiplicative de A, c'est-à-dire que S contient 1, et si $s, t \in S$, alors $st \in S$. On veut définir la *localisation* $S^{-1}A$ de A par rapport à S.

1. Montrer qu'on peut définir une relation d'équivalence sur $A \times S$ comme suit : (a, s) est équivalent à (b, t) s'il existe un $u \in S$ tel que $u(at - bs) = 0$. Soit $S^{-1}A$ l'ensemble des classes d'équivalences. On écrira $\frac{a}{s}$ pour désigner la classe d'équivalence de (a, s).
2. Montrer que $S^{-1}A$, muni des opérations $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$ et $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$, est un anneau commutatif.
3. Montrer que si S contient 0, alors $S^{-1}A$ est un anneau trivial.
4. Montrer que l'application $f : A \to S^{-1}A$ définie par $a \mapsto \frac{a}{1}$ est un morphisme d'anneaux. Montrer que f est injectif si S ne contient pas de diviseurs de zéro.
5. Cas particulier : corps des fractions. Supposons que A est intègre, et que $S = A \setminus \{0\}$. Montrer que $S^{-1}A$ est un corps, appelé le *corps des fractions* de A.
6. Cas particulier : localisation en un idéal premier. Soit P un idéal premier de A. Montrer que $S = A \setminus P$ est une partie multiplicative de A. On écrit A_P pour désigner $S^{-1}A$ dans ce cas.
7. Cas particulier (suite) : Montrer que l'idéal engendré par l'image de P dans A_P est le seul idéal maximal de A_P.

Exercice 3. Soit A un anneau factoriel. On suppose qu'il vérifie le théorème de Bezout, i.e. pour tous $a, b \in A$ premiers entre eux, il existe $u, v \in A$ avec $ua + vb = 1$.

1. Montrer que si $a, b \in A$ ont pour pgcd d, alors il existe $u, v \in A$ avec $ua + bv = d$.
2. Montrer que si une famille finie $a_1, \ldots, a_n$ d'éléments de A a pour pgcd 1, alors il existe des éléments $u_1, \ldots, u_n$ de A avec $\sum_{i=1}^{n} u_i a_i = 1$.
3. Montrer que si I est un idéal de A, alors il existe une famille finie d'éléments de I dont le pgcd est le pgcd de tous les éléments de I.
4. En déduire que A est principal.

Exercice 4. Soit $\mathbf{Z}[i]$ l'anneau des entiers de Gauß.

1. Soit p un nombre premier. Montrer que p est irréductible dans $\mathbf{Z}[i]$ si, et seulement si, p ne s'écrit pas comme somme de deux carrés d'entiers.
2. Soit p un nombre premier congru à 3 modulo 4. Montrer que si pour deux entiers a et b, on a $a^2 + b^2 \equiv 0 \mathrm{Mod} p$, alors p divise a et b.
   Indication : on pourra calculer $(p-1)!$ modulo p.
3. Montrer qu'une somme de deux carrés d'entiers est congrue à 0, 1 ou 2 modulo 4.
4. En déduire qu'un nombre premier p est irréductible dans $\mathbf{Z}[i]$ si, et seulement si, $p \equiv 3 \mathrm{Mod} 4$.

Exercice 5. Soit A le sous-anneau de $\mathbf{C}$ engendré par $\alpha = \frac{1+i\sqrt{19}}{2}$. Le but de cet exercice est de montrer que A est principal, mais pas euclidien.

1. Montrer d'abord que, si B est un anneau euclidien, alors il existe un élément non inversible $x \in B$ tel que la restriction à $B^* \cup \{0\}$ de la projection de B sur $B/(x)$ soit surjective.
   Ceci nous servira de critère pour montrer que l'anneau A n'est pas euclidien.
2. Donner un polynôme du second degré à coefficients entiers P s'annulant en α. En déduire que A est isomorphe à $\mathbf{Z}[X]/P$ et que le groupe abélien sous-jacent à A est engendré par 1 et α. Vérifier que l'application norme, qui à $z \in A$ associe $N(z) = z\overline{z}$, prend ses valeurs dans $\mathbf{N}$.
3. Montrer que 1 et -1 sont les seuls éléments inversibles de A.
4. Montrer qu'il n'existe pas de morphisme d'anneaux de A dans $\mathbf{Z}/2\mathbf{Z}$ ou $\mathbf{Z}/3\mathbf{Z}$.
   *Indication : pour chacun des deux cas, supposer que f soit un tel morphisme, et étudier l'image par f du polynôme trouvé en **2.***
5. En déduire que A n'est pas euclidien.
   *Indication : utiliser le critère de **1.***
6. On va montrer que A est principal.
   (a) Montrer que pour tout a, b éléments non nuls de A, il existe $q, r \in A$ tels que $r = 0$ ou $N(r) < N(b)$ et qui vérifient, soit $a = bq + r$, soit $2a = bq + r$.
   (b) Montrer que (2), l'idéal engendré par 2 dans A, est un idéal maximal de A.
   Indication : distinguer les cas où$y \in (2)$ et $y \notin (2)$.

(c) Montrer que l'idéal engendré par 2 est maximal dans A (on pourra utiliser le fait que A est isomorphe à un quotient de $\mathbf{Z}[X]$).

(d) Montrer que A est principal.

Exercice 6. Le *radical de Jacobson* d'un anneau commutatif A est l'intersection de tous les idéaux maximaux de A. On le note $\operatorname{rad} A$.

1. Soit A un anneau. Montrer qu'un élément a est dans le radical de A si, et seulement si, pour tout $x \in A$, $1 - ax$ est inversible.
2. Toujours en supposant que A est commutatif, montrer que si $x \in A$ est nilpotent, alors $1 - ax$ est inversible, pour tout élément $a \in A$.
3. Toujours dans le cas commutatif, montrer que le radical de A est le plus grand idéal de A tel que $1 - x$ est inversible pour tout $x \in \operatorname{rad} A$.
4. Toujours dans le cas où A est commutatif, soit I un idéal dont tous les éléments sont nilpotents. Montrer que $I \subseteq \operatorname{rad} A$.
5. Calculer le radical de $\mathbf{Z}$, $\mathbf{R}[X]$, $\mathbf{Z}/n\mathbf{Z}$ (pour un entier $n > 1$).

Exercice 7. Montrer qu'un polynôme $P(X, Y) \in \mathbf{Z}[X, Y]$ est tel que $P\big(t^2, t^3\big) = 0$ pour tout $t \in \mathbf{Z}$ si, et seulement si, il existe un polynôme $Q(X, Y) \in \mathbf{Z}[X, Y]$ tel que $P(X, Y) = (X^3 - Y^2) \cdot Q(X, Y)$. En déduire un isomorphisme de $\mathbf{Z}$-algèbres

$$\mathbf{Z}[X, Y]/\big(X^3 - Y^2\big) \cong \{P \in \mathbf{Z}[T] \ : \ P'(0) = 0\} \cong \mathbf{Z}[T^2, T^3].$$

Exercice 8 — Anneau local. Un anneau est dit *local* s'il n'admet qu'un seul idéal maximal.

1. Montrer que A est local si, et seulement si, l'ensemble de ses éléments non inversibles est un idéal et que, dans ce cas, cet idéal est l'unique idéal maximal.
2. Montrer que A est local si, et seulement si, pour tout élément $x \in A$, $1 - x$ ou x est inversible.
3. Un élément $x \in A$ est dit *idempotent* si $x^2 = x$. Montrer que si A est un anneau local, alors ses seuls idempotents sont 0 et 1. Donner un exemple d'anneau pour lequel la réciproque est fausse.
4. Soit k un corps et $n > 0$ un entier. Montrer que $k[X]/(X^n)$ est un anneau local et donner son idéal maximal.
5. Soit p un nombre premier, montrer que la localisation $\mathbf{Z}_{(p)}$ par rapport à l'idéal premier (p) est un anneau local et donner son idéal maximal.

Exercice 9. Soit $Q \in \mathbf{Z}[X]$ unitaire. On note $z_1, \ldots, z_n$ ses racines (pas forcément distinctes) dans $\mathbf{C}$. Montrer que

$$\prod_{i \neq j} (z_i - z_j) \in \mathbf{Z}.$$

Exercice 10. Soit k un corps. On note $F = k(X)$ le corps des fractions rationnelles.

1. Soient $R_1 = P_1/Q_1, \ldots, R_s = P_s/Q_s$ des éléments de F, avec $P_i \in k[X]$ et Q_i non nul dans $k[X]$ pour tout i de $\{1, \ldots, s\}$. Soit B la sous-k-algèbre de F engendrée par $R_1, \ldots, R_s$. Montrer qu'il existe un polynôme non nul $G \in k[X]$ tel que $B \subseteq (k[X])[G^{-1}]$.
2. En déduire que F n'est pas de type fini en tant que k-algèbre.

Exercice 11. Soient B un anneau, L un sous-anneau de B et A un sous-anneau de L. On suppose que L est un corps, que B est un L-espace vectoriel de dimension finie, et que B est aussi une A-algèbre de type fini. On se propose de montrer que L est une A-algèbre de type fini. Soient $\alpha_1, \ldots, \alpha_n$ dans B tels que $B = A[\alpha_1, \ldots, \alpha_n]$.

1. Soit $\beta_1, \ldots, \beta_m$ une base de B sur L, avec $\beta_1 = 1$. On écrit

$$\beta_i\beta_j = \sum_{k=1}^{m} a_{ijk}\beta_k; \quad \alpha_i = \sum_{j=1}^{m} b_{ij}\beta_j,$$

avec $a_{ijk}, b_{ij} \in L$. Soit C la sous A-algèbre de L engendrée par les a_{ijk} et les b_{ij}. Montrer que tout élément x de B s'écrit :

$$x = \sum_{i=1}^{m} \lambda_i\beta_i,$$

où les λ_i sont dans C.

2. En déduire que $L = C$, et conclure.

Exercice 12 — Lemme de Zariski. Cet exercice utilise les exercices 10 et 11. Soient $k \subset K$ deux corps, tels que K soit une k-algèbre de type fini. Le but de l'exercice est de montrer que K est un k-espace vectoriel de dimension finie. Pour cela on écrit $K = k[\alpha_1, \ldots, \alpha_n]$, et on raisonne par récurrence en supposant le résultat vrai jusqu'à $n - 1$, le cas $n = 0$ étant trivial.

1. On pose[1] $L = k(\alpha_1)$. Comparer K et $L[\alpha_2, \ldots, \alpha_n]$, et en déduire que K est de dimension finie sur L.

1. C'est le corps des fractions de $k[\alpha_1]$.

2. En utilisant l'exercice 11, montrer que L est une k-algèbre de type fini.
3. En utilisant l'exercice 10, montrer que α_1 est racine d'un polynôme unitaire de $k[X]$, puis que L est de dimension finie sur k.
4. En déduire le résultat annoncé.

Exercice 13 — Théorème des zéros de Hilbert. Cet exercice utilise le résultat de l'exercice 12. Soit k un corps.

1. Soient $a_1, \ldots, a_n$ dans k. Montrer que le morphisme $u : P \mapsto P(a_1, \ldots, a_n)$ de $k[X_1, \ldots, X_n]$ dans k est surjectif de noyau l'idéal $J = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$.

   On suppose dans la suite que k est algébriquement clos et on se donne I un idéal maximal de $k[X_1, \ldots, X_n]$.
2. Montrer que le corps $L = k[X_1, \ldots, X_n]/I$ est isomorphe (en tant que k-algèbre) à k.
   Indication : On appliquera le résultat principal de l'exercice 12.
3. En déduire qu'il existe $a_1, \ldots, a_n$ dans k tel que I soit l'idéal J du **1.**, c'est-à-dire que I est l'ensemble des polynômes $P \in k[X_1, \ldots, X_n]$ tels que $P(a_1, \ldots, a_n) = 0$.

Exercice 14. Montrer que les polynômes suivants sont irréductibles.

1. Pour $n > 0$ et p premier, $X^n - p$ sur $\mathbf{Q}$;
2. $X^4 + X + 1$ sur $\mathbf{Q}$;
3. $X^6 + X^2 + 1$ sur $\mathbf{Q}$;
4. Pour $n > 0$, $X^n - T$ sur $K(T)$ (K un corps);
5. $1 + X + \cdots + X^{p-1}$ sur $\mathbf{Q}$, pour p premier.