TD n°4.

1 Anneaux factoriels

Exercice 1. Soit A un anneau intègre vérifiant la condition (E) d'existence d'une décomposition de tout élément en produit de facteurs irréductibles. Montrer l'équivalence des propositions suivantes :

a) A vérifie l'unicité de la décomposition (c'est-à-dire A est factoriel) ;

b) si p est irréductible, et p divise ab, alors p divise a ou b (lemme d'Euclide) ;

c) p est irréductible si et seulement si (p) est un idéal premier ;

d) si a divise bc et si a est premier avec b, alors a divise c (théorème de Gauss).

Exercice 2. Soit A un anneau factoriel et $a \in A$. Montrer que $\sqrt{aA}$ est un idéal principal.

Exercice 3. Contenus
A désigne un anneau factoriel. On note $c(P)$ pour $P \in A[X]$, le contenu de P : c'est le pgcd de ses coefficients. P est primitif si $c(P)$ est inversible. On note $k = \mathrm{Frac}(A)[X]$.

a) Soit p premier un élément de A qui divise $P \cdot Q \in A[X]$. Montrer que p divise P ou Q. (Lemme de Gauss)

b) i) Montrer que, si P et Q sont primitifs, alors PQ est primitif

ii) Montrer que $c(P)c(Q) = c(PQ)$

c) Monrter que, si P primitif divise Q dans $k[X]$, alors P divise Q.

d) Montrer que $P \in A[X]$ est irréductible si et seulement si il est primitif et irréductible dans $k[X]$.

Exercice 4. Critère d'irréductibilité d'Eisenstein

a) soit A un anneau factoriel et K son corps des fractions. Soit $f = \sum_{i=0}^{d} a_i X^i \in A[X]$ un polynômes de degré $d \geq 1$. Soit p un élément irréductible de A. Supposons que p ne divise pas a_d, que p divise a_i pour $0 \leq i < d$ et que p^2 ne divise pas a_0. Montrer que f est irréductible dans $K[X]$.

b) Montrer que $X^4 + X^2Y^3 + Y$ est irréductible dans $\mathbb{Q}[X, Y]$.

c) Soient A est un anneau intègre et $\mathfrak{p}$ un idéal premier Soit $f = \sum_{i=0}^{d} a_i X^i \in A[X]$ un polynômes de degré $d \geq 1$ tel qu'aucun élément non inversible ne divise tous les coefficients. Supposons $a_d \notin \mathfrak{p}$, $a_i \in \mathfrak{p}$ pour $0 \leq i < d$ et que $a_0 \notin \mathfrak{p}^2$. Montrer que f est irréductible dans $A[X]$.

Exercice 5. Soit A un anneau intègre et K son corps de fractions. On dit que $x \in K$ est entier sur A si $A[x]$ est un A-module de type fini. On dit que A est intégralement clos si tout élément de K entier sur A est dans A.

a) Montrer que $x \in K$ est entier sur A si et seulement si il existe un polynôme unitaire de $A[X]$ dont x est racine.

b) Montrer que si A est factoriel, alors A est intégralement clos.

Exercice 6. Montrer que $A = k[X, Y]/(X^2 - Y^3)$ est intègre et s'identifie à un sous-anneau de $k[T]$.

Exercice 7. Déterminer les décompositions en facteurs irréductibles de
(i) 120 dans le localisé $S^{-1}\mathbb{Z}$ avec $S = \{1, 2, 2^2, \cdots, 2^n, \cdots\}$.
(ii) 120 dans le localisé $S^{-1}\mathbb{Z}$ avec $S = \mathbb{Z} - (2)$, i.e. le localisé de $\mathbb{Z}$ en l'idéal premier (2).
(iii) $X^2Y^2 - X^3 - Y^3 + XY$ dans $\mathbb{C}[X, Y]$.
(iv) $-X^2Y + X^2Z + XY^2 - XZ^2 - Y^2Z + YZ^2$ dans $\mathbb{Q}[X, Y, Z]$.
(v) $X^n - Y$ dans $k[X, Y]$ où k est un corps.
(vi) $X^n + Y^n - 1$ dans $k[X, Y]$ où k est un corps.
(vii) $a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ dans $k[a_0, \cdots, a_n, X]$ où k est un corps.

Exercice 8. Montrer que le polynôme $X_1^2 + \cdots + X_n^2$ est irréductible pour $n \geq 2$ dans $\mathbb{R}[X_1, \cdots, X_n]$ et pour $n \geq 3$ dans $\mathbb{C}[X_1, \cdots, X_n]$.

Exercice 9. Soit $P = a_n X^n + \cdots + a_0$ un élément de $\mathbb{Z}[X]$. Et soit $r = \frac{p}{q} \in \mathbb{Q}$ une racine de P

a) $qX - p$ divise P.

b) i) En déduire que $p|a_0$

ii) En déduire que $q|a_n$

iii) En déduire que $p - q|P(1)$

iv) En déduire que $p + q|P(-1)$.

c) Trouver les racines rationelles de $A(x) = x^3 - 6x^2 + 15x - 14$ et $B(x) = x^4 - 2x^3 - 8x^2 + 13x - 24$.

Exercice 10. Soit n un entier premier à 10. Montrer que la suite des nombres 1, 11, 111, 1111, ... contient une infinité de multiples de n. Est-ce encore vrai pour la suite 17, 1717, 171717, ... ?

Exercice 11. Trouver le pgcd et les coefficients de Bézout correspondants de $n - 1$ et $n + 1$ ainsi que ceux de $n^2 + 1$ et $n^3 - n$.

Exercice 12. Résolution de $3^m - 2^n = 1$

a) En raisonnant modulo 4, montrer que m est pair ou vaut 1.

b) si $m \neq 1$, $3^{m/2} - 1$ et $3^{m/2} + 1$ sont des puissances de 2.

c) Trouver les solutions de $3^m - 2^n = 1$.

Exercice 13. À quelle condition $X^m + 1$ divise $X^n + 1$?

a) Déterminer le PGCD de $X^7 - a$ et $X^5 - b$.

b) si $a^5 = b^7$, $X^7 - a$ et $X^5 - b$ ont une racine commune. La déterminer.

c) Soit $P = X^2 + 1$ et $Q = X^3 + 1$. Déterminer le PGCD de P et Q. Quels sont les polynômes U et V vérifiant $UP + VQ = 1$?

Exercice 14. a) Trouver un pgcd de $X^6 - 1$ et de $X^4 - 1$ dans $\mathbb{C}[X]$, par factorisation et par l'algorithme d'Euclide.

b) Résoudre dans $\mathbb{C}[X]^2$, l'équation $P(X)(X^6 - 1) + Q(X)(X^4 - 1) = X^3 + 2X^2 - X - 2$.

c) Résoudre la même équation dans $\mathbb{R}[X]$.

Exercice 15. Factorisations et congruences

a) Soit $P(X) = X^4 + 1$. Décomposer P dans $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$ en produits de facteurs irréductibles.

b) Montrer que $-1, 2$ ou -2 est un carré dans $\mathbb{F}_p$ pour tout p.

c) Montrer que $X^4 + 1$ est factorisable dans $\mathbb{F}_p$ (on utilisera les égalités $X^4 + 1 = (X^2 + 1)^2 - 2X^2 = (X^2 - 1)^2 + 2X^2 = (X^2)^2 - (-1)$).

d) Factoriser $Q(X) = X^5 - X - 1$ dans $\mathbb{F}_5[X]$ (on vérifiera que si x est un élément d'une extension de degré 2 de $\mathbb{F}_5$, alors $x^{25} = x$) et en déduire que $X^5 - X - 1$ est irréductible dans $\mathbb{Q}[X]$.

e) Montrer que $X^5 - X^2 - 1$ est irréductibles dans $\mathbb{Q}[X]$.

Exercice 16. Quels sont les polynômes irréductibles de degré inférieur à 4 dans $\mathbb{F}_2[X]$.

Exercice 17. Exemple de polynôme irréductible
$P(x) = (x - a_1) \cdots (x - a_n) - 1$ est irréductible sur $\mathbb{Q}$ si les a_i sont des entiers distincts.

Exercice 18. Eléments étrangers conservants le ppcm
n et m désignent deux éléments d'un anneau A factoriel.

a) Montrer qu'il existe $n'|n$ et $m'|m$, tels que $(n', m') = 1$ et $\text{ppcm}(n', m') = \text{ppcm}(n, m)$.

b) si n' et m' répondent au problème et si $d = (n, m)$, alors tout p irréductible qui divise m/d divise m' et ne divise pas n'.

c) En déduire un algorithme qui calcule n' et m' en effectuant uniquement des calculs de pgcd et des divisions euclidiennes.

Exercice 19. a) Soit R un anneau euclidien. Montrer qu'il existe $x \in R$ non inversible tel que $R^* \cup \{0\} \to R/(x)$ soit surjective.

b) Soit $A = \mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$. Déterminer A^* et montrer que A n'est pas euclidien.

c) Soit $x \in \mathbb{C}$. On veut montrer qu'il existe $q \in A$ tel que $|x-q| < 1$ ou $|2x-q| < 1$. On pose $x = u + iv$ avec $u, v \in \mathbb{R}$.

i) Se ramener au cas où $v \in [0, \sqrt{19}/4]$.

ii) Montrer que si $v \in [0, \sqrt{3}/2[$, il existe $q \in \mathbb{Z}$ tel que $|x-q] < 1$.

iii) Montrer que si $v \in [\sqrt{3}/2, \sqrt{19}/4]$, $\sqrt{19}/2 - 2v \in [0, \sqrt{3}/2[$ et en déduire $q \in A$ tel que $|2x-q| < 1$.

d) Soient $a, b \in A \backslash 0$. Montrer qu'il existe $q, r \in A$ tels que $r = 0$ ou $|r| < |b|$ et qui vérifient, soit $a = bq + r$, soit $2a = bq + r$.

e) Montrer que (2) est un idéal maximal de A (on pourra soit écrire la table de multiplication de $A/(2)$, soit vérifier que $X^2 + X + 5$ est un polynôme irréductible de $\mathbb{Z}/(2)[X]$).

f) Soit I un idéal de A et $b \in I - \{0\}$ minimisant $|b|$. Montrer que $2I \subset (b) \subset I$.

g) Montrer que A est principal.

2 Compléments à la feuille de TD 3

Exercice 20. Un A-module M est dit artinien si toute suite décroissante de sous-A-modules de M est stationnaire. Un anneau A est dit artinien si il est artinien en tant que A-module.

a) Montrer qu'un A-module M est artinien si et seulement si toute famille de sous-module de M admet un élément minimal.

b) Soit k-un corps. Montrer qu'une algèbre de dimension finie sur k est artinienne.

c) Soit N un sous-module de M. Montrer que M est artinien si et seulement si N et M/N sont artiniens.

d) Montrer qu'un anneau intègre est artinien si et seulement si c'est un corps.

e) Soit k un corps. Montrer qu'un k-espace vectoriel M est un k-module artinien si et seulement si il est de dimension fini.

f) On suppose dorénavant que A est un anneau artinien.

i) Montrer que tout idéal premier de A est un idéal maximal.

ii) Montrer que A n'a qu'un nombre fini d'idéaux maximaux (on pourra utiliser le lemme chinois ou un argument de comaximalité).

iii) Si $\mathfrak{m} \in \mathrm{Spec}(A)$, on note $\mathfrak{m}^\infty = \bigcap_{n\in\mathbb{N}} \mathfrak{m}^n$ et $k_\mathfrak{m} = A/\mathfrak{m}$. Munir $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ d'une structure de $k_\mathfrak{m}$-espace vectoriel et montrer qu'il est de dimension finie. En déduire que $A/\mathfrak{m}^\infty$ est un anneau noethérien.

iv) Montrer que $A \to \prod_{\mathfrak{m}\in\mathrm{Spec}(A)} A/\mathfrak{m}^\infty$ est surjective. Soit $\mathfrak{R}^\infty$ le noyau de ce morphisme. Montrer que $\mathfrak{R}^\infty \cdot \mathfrak{m} = \mathfrak{R}^\infty$ pour tout idéal maximal $\mathfrak{m}$ de A. Soit $J = \mathrm{Ann}(\mathfrak{R}^\infty) = \{x \in A, \forall y \in \mathfrak{R}^\infty, xy = 0\}$.

v) On suppose $J \neq A$. Montrer qu'il existe un idéal J' contenant J tel que J'/J soit un A-module simple et, en utilisant la question 2 de l'exercice 2, en déduire qu'il existe un idéal maximal $\mathfrak{m}$ de A tel que $J'\mathfrak{m} \subset J$. En déduire que $J' \subset \mathrm{Ann}(\mathfrak{R}^\infty)$ et obtenir une contradiction.

vi) En déduire que $A \to \prod_{\mathfrak{m}\in\mathrm{Spec}(A)} A/\mathfrak{m}^\infty$ est un isomorphisme. Montrer que A est un anneau noetherien.

g) Réciproquement soit A un anneau noethérien dont tout idéal premier est maximal.

i) Montrer qu'il existe un sous-module de A maximal M pour la propriété d'être artinien.

ii) Soit $a \in A - M$, montrer que $M + (a)$ et $M + (a)/M$ sont artiniens et en déduire une contradiction. En déduire que A est artinien.

Exercice 21. Un A-module est dit simple si il a exactement deux sous-modules (0 et lui-même). Un A-module M est dit de longueur finie si il existe une suite de sous-modules

$$0 = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_m = M$$

telle que, pour tout $1 \leq i \leq n$, M_i/M_{i-1} soit simple (une tel suite est appelé suite de décomposition de M et les M_i/M_{i-1} sont).

a) Soit I un idéal de A. Montrer que A/I est un A-module simple si et seulement si I est un idéal maximal.

b) Soit M un module simple. Montrer qu'il existe un idéal maximal $\mathfrak{m}$ tel que M soit isomorphe à $A/\mathfrak{m}$.

c) Montrer que si M est un module de type fini non nul, alors M a un sous-module N tel que M/N soit simple.

d) Montrer qu'un A-module est de longueur fini si et seulement si il est noethérien et artinien.

e) Montrer que si M est de longueur fini, la longueur m de la suite de décomposition ne dépend pas du choix de la suite de décomposition et que les facteurs non plus à permutation près. Plus précisément, si

$$0 = N_0 \subset N_1 \subset N_2 \subset \cdots \subset N_n = M$$

est une autre suite de décomposition, montrer que $m = n$ et qu'il existe $\sigma \in \mathfrak{S}_n$ tel que M_i/M_{i-1} soit isomorphe à $N_{\sigma(i)}/N_{\sigma(i)-1}$.

Exercice 22. Soit A un anneau local, d'anneau local, d'idéal maximal $\mathfrak{m}$. Soit $k = A/\mathfrak{m}$

a) Soit P un A-module projectif (cf. TD 3 exo 9) de type fini.

b) Montrer qu'il existe $n \in \mathbb{N}$ et un A-module de type fini P' tel que $P \oplus P' \simeq A^n$. On identifie dorénavant $P \oplus P'$ et A^n.

c) Munir $P/\mathfrak{m}P$ et $P'/\mathfrak{m}P'$ d'une structure de k-espace vectoriel. Soit $(\bar{e}_i)_{i\in I}$ et $(\bar{e}'_j)_{j\in J}$ une base de $P/\mathfrak{m}P$ et $P'/\mathfrak{m}P'$ respectivement. Montrer que $\mathrm{Card}(I) + \mathrm{Card}(J) = n$

d) Soit e_i un antécédent de $\bar{e}_i$ par le morphisme $P \to P/\mathfrak{m}P$ et e'_j un antécédent de $\bar{e}'_j$ par le morphisme $P' \to P'/\mathfrak{m}P'$. Montrer que $(e_i)_{i\in I}$ et $(e'_j)_{j\in J}$ sont des familles génératrices de P et P' (on pourra appliquer le lemme de Nakayama (TD 2 exo 13) à $P/\langle e_i\rangle_{i\in I}$).

e) En déduire deux applications surjectives $A^{\mathrm{Card}(I)} \to P$ et $A^{\mathrm{Card}(J)} \to P'$. En déduire une application surjective $f : A^n \to A^n$.

f) Montrer que $\det f$ est inversible (on pourra réduire modulo $\mathfrak{m}$). Montrer que f est un isomorphisme.

g) En déduire que P est un module libre.

Exercice 23. Soit A l'anneau des fonctions continues de $\mathbb{R}$ vers $\mathbb{R}$ qui sont π-périodiques. Soit $P = \{g \in \mathcal{C}^0(\mathbb{R},\mathbb{R}), g(x+\pi) = -g(x)\}$.

a) Munir P d'une structure de A-module via $(f.g)(x) = f(x)g(x)$.

b) Montrer que $\Big((\cos,\sin),(\sin,-\cos)\Big)$ forme une base du A-module $P \oplus P$.

c) Montrer que P n'est pas un A-module libre (on pourra commencer par montrer que toute famille d'au moins deux éléments de P est liée).