TD n°3.

Exercice 1. Soit A un anneau.
Montrer que $A[\mathbb{Z}]$ est isomorphe à $A[X,Y]/(XY-1)$.
Soit $n \geq 1$ un entier. Montrer que $A[\mathbb{Z}/n\mathbb{Z}]$ est isomorphe à $A[X]/(X^n-1)$.

Exercice 2. Soit A un anneau non nul. Soit $B = A[\mathbb{N}^n]$, on note $S = \{e_\nu, \nu \in \mathbb{N}^n\} \subset B$ (S est une partie multiplicative de B). Montrer que $S^{-1}B$ est isomorphe à $A[\mathbb{Z}^n]$.

Exercice 3. Soit $A = \mathbb{C}[\mathbb{Z}]$. On notera $X = e_1$.

a) Montrer que tout élément a non nul de A peut s'écrire de façon unique sous la forme $a = X^m P(X)$ où $m \in \mathbb{Z}$ et P est un polynôme de terme constant non nul. On note $e(a) = \deg(P)$.
b) Soient $a, b \in A$ montrer qu'il existe $q, r \in A$ tels que $a = bq + r$ et : $r = 0$ ou $e(r) < e(b)$.
c) En déduire que A est principal.

Exercice 4. Montrer que dans un anneau principal A, les idéaux premiers sont maximaux.

Exercice 5. Soit A un anneau factoriel et $a \in A$. Montrer que $\sqrt{aA}$ est un idéal principal.

Exercice 6. 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 7. 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 8. 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 9. Montrer que $A = k[X,Y]/(X^2 - Y^3)$ est intègre et s'identifie à un sous-anneau de $k[T]$.
Montrer que A n'est pas intégralement clos (et donc en particulier n'est pas factoriel).

Exercice 10. 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 11. 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 12. 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 13. 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 14. Soit p un nombre premier.
Montrer que $\mathbb{Z}[i]/(p)$ est isomorphe à $\mathbb{F}_p[X]/(X^2 + 1)$.
EN déduire que p est irréductible dans $\mathbb{Z}[i]$ si et seulement si -1 n'est pas un carré dans $\mathbb{F}_p$.

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. Montrer que $P(X) = (X - a_1) \cdots (X - a_n) - 1$ est irréductible dans $\mathbb{Q}[X]$ si les a_i sont des entiers distincts.

Exercice 18. 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.