Feuille de TD 2
Complément sur les anneaux (suite)

Corps de fractions

Exercice 1 (Sur la définition du corps de fractions)
Soient A un anneau commutatif intègre et L un corps contenant A tel que tout élément de L est de la forme as^{-1} avec $a \in A$ et $s \in A \setminus \{0\}$. Montrer que L est canoniquement isomorphe à $\mathrm{Fr}(A)$.

Exercice 2 (Exemples de corps de fractions)
Déterminer le corps des fractions des anneaux suivants : $\mathbb{Z}[X]$, $\mathbb{Z}[i]$, $\mathbb{Z}[1/2]$, $k[X^2, X^3]$ (où k est un corps) et $\{P \in \mathbb{Q}[X] : P(0) \in \mathbb{Z}\}$.

Exercice 3 (Fractions rationnelles symétriques)
Soit k un corps et $n \geq 2$.

1. Montrer que l'action de $\mathbb{S}_n$ sur $k[X_1, \ldots, X_n]$ s'étend naturellement à une action par automorphismes de corps sur $k(X_1, \ldots, X_n)$.
2. Montrer que le sous-corps L des fractions rationnelles invariantes par $\mathbb{S}_n$ est égal au corps des fractions de $k[X_1, \ldots, X_n]^{\mathbb{S}_n}$. *Indication :* si P/Q est symétrique, c'est-à-dire invariante par $\mathbb{S}_n$, poser $D = \prod_{\sigma \in \mathbb{S}_n} (\sigma \cdot Q)$.

Exercice 4 (Décomposition en éléments simples de fractions rationnelles $*$)
Soit k un corps.

1. Soient $n \geq 1$ et $P/Q \in k(X)$ une forme irréductible non nulle avec $Q = \prod_{i=1}^n Q_i$ où les polynômes Q_i sont non constants deux à deux premiers entre eux. Montrer qu'il existe $P_1, \ldots, P_n$ tels que $P/Q = \sum_{i=1}^n P_i/Q_i$ avec P_i et Q_i premiers entre eux pour tout $i \in \{1, \ldots, n\}$.
2. Soient S et Q dans $k[X]$ avec $Q \neq 0$. Montrer qu'il existe $S_0, \ldots, S_{n-1}$ et R_n des polynômes tels que $S = \sum_{j=0}^{n-1} S_j Q^j + R_n Q^n$ et $\deg S_\ell < \deg Q$ pour tout $0 \leq \ell \leq n-1$.
3. En déduire que si $F \in k(X)$ s'écrit sous forme irréductible P/Q avec Q de factorisation en irréductibles distincts $Q = \prod_{i=1}^n Q_i^{\alpha_i}$ ($\alpha_i \in \mathbb{N}^*$), alors
$$F = E + \sum_{i=1}^n \sum_{j=1}^{\alpha_i} \frac{P_{i,j}}{Q_i^j} \text{ avec } E \in k[X] \text{ et } 0 \leq \deg P_{i,j} < \deg Q_i \text{ pour tout } i, j.$$

Anneaux factoriels

Exercice 5
Soit A un anneau commutatif tel que $A[X]$ est factoriel. Montrer que A est factoriel.

Exercice 6
Soit A un anneau factoriel et $K = \mathrm{Fr}(A)$ son corps des fractions. Soient $P, Q \in A[X]$ avec Q primitif. Montrer que si $Q|P$ dans $K[X]$, alors $Q|P$ dans $A[X]$.

Exercice 7

1. ($*$) Soient $n \in \mathbb{N}$ et $p \in \mathbb{N}$ premier.
   (i) Montrer que la valuation p-adique de $n!$ est donnée par
   $$v_p(n!) = \sum_{\ell \geq 1} \left\lfloor \frac{n}{p^\ell} \right\rfloor.$$
   (ii) Soit $(n_N, \ldots, n_0)_p$ l'écriture de n en base p, *i.e.* on a $n = \sum_{\ell=0}^N n_\ell p^\ell$ avec $n_\ell \in \{0, \ldots, p-1\}$. Montrer que
   $$v_p(n!) = \frac{n-s}{p-1}, \text{ avec } s = \sum_{\ell=0}^N n_\ell.$$
   (iii) Utiliser les formules précédentes pour montrer que les coefficients binomiaux sont des entiers.

2. Soit A un anneau factoriel et $a, b, c \in A$ non nuls tels que $a + b + c = 0$. Étant donné π un irréductible de A, montrer qu'au moins deux éléments parmi a, b et c ont la même valuation π-adique.

3. Résoudre dans $\mathbb{Z}^3$ l'équation $x^3 + 2y^3 + 4z^3 = 0$.

Exercice 8
Soit A un anneau factoriel et soient $a \in A \setminus \{0\}$ et $m \geq 2$. Montrer que si $a^m = uv$ avec u et v premiers entre eux dans A, alors il existe $c, d \in A^\times$ et $\bar{u}, \bar{v} \in A$ tels que $u = c\bar{u}^m$ et $v = d\bar{v}^m$.

Exercice 9 (Une équation diophantienne)
On souhaite résoudre l'équation $y^3 - x^2 = 2$ dans $\mathbb{Z}$.

1. En utilisant la même méthode que pour les entiers gaussiens, montrer que $\mathbb{Z}[i\sqrt{2}]$ est euclidien (donc factoriel) et déterminer ses éléments inversibles.

2. Soit $(x, y) \in \mathbb{Z}^2$ une solution de l'équation $y^3 - x^2 = 2$. Montrer que $x + i\sqrt{2}$ et $x - i\sqrt{2}$ sont premiers entre eux dans $\mathbb{Z}[i\sqrt{2}]$. En déduire que $x + i\sqrt{2}$ et $x - i\sqrt{2}$ sont des cubes dans $\mathbb{Z}[i\sqrt{2}]$. Conclure.

Exercice 10

1. Soit $P \in k[X]$ un polynôme unitaire de degré $d \geq 1$ à coefficients dans un corps k.
   (i) On suppose dans cette question que k est de caractéristique nulle. Montrer que P et P' sont premiers entre eux si et seulement P est sans facteur carré (de degré supérieur ou égal à 1). En déduire que P n'a que de racines simples dans toute extension de k si et seulement si P et P' sont premiers entre eux.
   (ii) Si k est de caractéristique p, montrer que si $Q \in k[X]$ est de dérivée nulle, alors il existe un polynôme $S \in k[X]$ tel que $Q(X) = S(X^p)$. En déduire que l'équivalence précédente est remplacée par :
   $$P \text{ et } P' \text{ premiers entre eux ssi } P \text{ sans facteur carré et sans facteur du type } S(X^p).$$

2. Soit $P \in \mathbb{Q}[X]$ irréductible. Que peut-on dire de la multiplicité de ses racines dans $\mathbb{C}$?

3. Soient $R_1, R_2 \in \mathbb{Q}[X]$ irréductibles unitaires. Montrer que s'il existe $\alpha \in \mathbb{C}$ tel que $R_1(\alpha) = R_2(\alpha) = 0$, alors $R_1 = R_2$.

4. Soit $P = (X - a)^3(X - b)^2(X - c) \in \mathbb{Q}[X]$ avec $a, b, c \in \mathbb{C}$ distincts. Montrer que $a, b, c \in \mathbb{Q}$.

Exercice 11
Soit $P \in \mathbb{R}[X]$. Montrer que les conditions suivantes sont équivalentes:

(i) pour tout $x \in \mathbb{R}$, $P(x) \geq 0$;

(ii) il existe $A, B \in \mathbb{R}[X]$ tels que $P = A^2 + B^2$.

Exercice 12
La notion de factorialité généralise la propriété de décomposition unique en facteurs premiers de $\mathbb{Z}$ mais cela ne veut pas dire que les anneaux factoriels vérifient toutes les propriétés de $\mathbb{Z}$. On considère un corps k.

1. Montrer que $k[X, Y]$ et $\mathbb{Z}[X]$ sont des exemples d'anneaux factoriels qui ne sont pas de Bézout (on rappelle qu'un *anneau de Bézout* est un anneau intègre tel que tout idéal de type fini est principal).

2. Montrer que l'anneau $k[X_i : i \in \mathbb{N}] = \cup_{i \in \mathbb{N}} k[X_0, \ldots, X_n]$ est factoriel.

Exercice 13 ($*$)
Soit A un anneau commutatif intègre. On rappelle qu'un élément $x \in \mathrm{Fr}(A)$ est *entier* sur A s'il existe un polynôme unitaire $Q \in A[X]$ tel que $Q(x) = 0$. On dit que A est *intégralement clos* si tout élément $x \in \mathrm{Fr}(A)$ qui est entier sur A appartient à A.

1. Montrer que tout anneau factoriel est intégralement clos.

2. Soit $d \in \mathbb{Z}^*$ un entier sans facteur carré. Montrer que si $d = 1 \pmod 4$, alors $\mathbb{Z}[\sqrt{d}]$ n'est pas intégralement clos (donc non factoriel). *Indication* : considérer l'élément $(1 + \sqrt{d})/2$.

Exercice 14
Montrer que $\mathbb{Z}[i\sqrt{d}]$ n'est jamais factoriel si $d \geq 3$. On montrera que le lemme d'Euclide n'est pas satisfait en remarquant que $2|(d + i\sqrt{d})(d - i\sqrt{d})$.

Exercice 15 (Exemples d'anneaux non factoriels)

1. Dans $\mathbb{Z}[i\sqrt{3}]$, montrer que 4 et $2(1+i\sqrt{3})$ n'ont ni PPCM ni PGCD. La fraction $4/2(1+i\sqrt{3})$ admet-elle une unique forme irréductible dans $\mathrm{Fr}(\mathbb{Z}[i\sqrt{3}])$?

2. Montrer que $A = \{P \in \mathbb{Q}[X] : P(0) \in \mathbb{Z}\}$ n'est pas factoriel.

Exercice 16
On considère le morphisme de $\mathbb{C}$-algèbres $\phi : \mathbb{C}[X,Y,Z] \to \mathbb{C}[U,V]$ défini par $\phi(X) = U^2$ et $\phi(Y) = V^2$ et $\phi(Z) = UV$.

1. Le morphisme ϕ est-il surjectif?

2. Montrer que le noyau de ϕ est l'idéal de $\mathbb{C}[X,Y,Z]$ engendré par $XY - Z^2$.

3. Montrer que l'anneau quotient $A = \mathbb{C}[X,Y,Z]/(XY - Z^2)$ est intègre.

4. Montrer que l'élément $\bar{X}$ de A est un irréductible de A.

5. L'anneau quotient $\mathbb{C}[X,Y,Z]/(XY - Z^2)$ est-il factoriel?

6. Montrer que $(\bar{X}, \bar{Z})$ est un idéal premier de A qui contient $\bar{X}$.

7. Les éléments $\bar{X}$ et $\bar{Z}$ ont-ils un PGCD dans A?

8. Les éléments $\bar{X}$ et $\bar{Z}$ ont-ils un PPCM dans A?

Exercice 17 (*)
Montrer qu'un anneau factoriel et de Bézout est principal.

Exercice 18
Donner toutes les implications entre les propriétés suivantes, où A est un anneau commutatif intègre :

1. A est euclidien;
2. A est principal;
3. A est factoriel;
4. A est un anneau de Bézout;
5. A est à PGCD;
6. A vérifie la propriété D[1];
7. A vérifie la propriété AP[2];
8. A est atomique;
9. A est factoriel sans restriction[3].

Exercice 19
Étudier l'irréductibilité des polynômes dans $\mathbb{Q}[X,Y]$: $Y - X^2$, $X^2 + Y^2 - 1$, $X^2 + Y^2 + 1$, $X^2 - Y^2 - 1$, $Y^2 - X^3$, $X^3 - Y^2 - X$, $XY^3 - X^2Y - Y^2 + X$.

Exercice 20

1. Soit $p \in \mathbb{N}$ un nombre premier. Montrer que le polynôme $X^{p-1} + \cdots + X + 1$ est irréductible sur $\mathbb{Z}[X]$. *Indication* : poser $X = Y + 1$ et appliquer le critère d'Eisenstein avec p.

2. Soit $A = \mathbb{Z}[T]$. Montrer que le polynôme $X^n - T \in A[X]$ est irréductible.

Exercice 21
Étudier l'irréductibilité des polynômes suivants sur $\mathbb{Z}$ en les réduisant modulo des nombres premiers : $X^3 + 4X^2 - 5X + 7$, $5X^3 + 3X^2 - 4X - 27$, $X^3 - 6X^2 - 4X - 13$, $X^3 + 4X^2 - 4X + 25$, $X^4 + 5X^3 - 3X^2 - X + 7$, $X^4 + 7X^2 + 4X + 1$, $X^6 + X^3 + 1$, $X^7 + X + 1$.

Exercice 22
Soit $P(X) = X^4 + 1 \in \mathbb{Z}[X]$.

1. Montrer que P est irréductible sur $\mathbb{Z}$.
   Indication : calculer $P(X+1)$ et appliquer le critère d'Eisenstein avec $p = 2$.

2. Montrer que P est réductible modulo 2, puis pour tout p premier impair.

---

[1] On rappelle qu'un anneau A intègre satisfait la *propriété D* si pour tout $a, b, c \in A \setminus \{0\}$, tels que $a|(bc)$ et a et b sont premiers entre eux (*i.e.* si $d|a$ et $d|b$, alors $d \in A^\times$), alors $a|c$.

[2] On rappelle qu'un anneau A intègre satisfait la *propriété AP* si tout élément irréductible de A est premier.

[3] On rappelle qu'un anneau A intègre est *factoriel sans restriction* si toute égalité $x_1 \dots x_n = y_1 \dots y_m$, avec x_i, y_j irréductibles de A pour tous $i \in \{1, \dots, n\}$ et $j \in \{1, \dots, m\}$, implique que $n = m$ et qu'il existe une permutation $\sigma \in \mathbb{S}_n$ telle que x_i et $y_{\sigma(i)}$ sont associés pour tout $i \in \{1, \dots, n\}$.