G1. ALGÈBRE COMMUTATIVE.

UNIVERSITÉ DE RENNES 1

Feuille d'exercice n° 2: Idéaux premiers, maximaux; anneaux principaux, factoriels

A. CHAMBERT-LOIR, P. AUTISSIER, D. FERRAND

A. ANNEAUX DE FRACTIONS

EXERCICE 1

Soit A un anneau commutatif et soit S une partie multiplicative de A.

1 Montrer que l'homomorphisme canonique $i : A \to S^{-1}A$ est injectif si et seulement si tout élément de S est simplifiable.

2 Plus généralement, déterminer le noyau de l'homomorphisme i.

EXERCICE 2

Soit A un anneau commutatif et soit S une partie multiplicative de A.

1 Quels sont les éléments inversibles de l'anneau des nombres décimaux ?

2 Montrer qu'un élément $a \in A$ est inversible dans $S^{-1}A$ si et seulement s'il existe $b \in A$ tel que $ab \in S$.

3 Si T est une partie multiplicative de A qui contient S, construire un homomorphisme d'anneaux de $S^{-1}A$ dans $T^{-1}A$.

4 Soit $\tilde{S}$ l'ensemble des éléments de A dont l'image est inversible dans $S^{-1}A$. Montrer que l'homomorphisme d'anneaux canonique de $S^{-1}A$ dans $\tilde{S}^{-1}A$ est un isomorphisme. On donnera une démonstration explicite ainsi qu'une démonstration utilisant la propriété universelle.

EXERCICE 3

1 Soit A un sous-anneau de $\mathbf{Q}$. Montrer qu'il existe une partie multiplicative S de $\mathbf{Z}$ telle que $A = S^{-1}\mathbf{Z}$.

2 Soit $A = \mathbf{C}[X, Y]$ l'anneau des polynômes en deux indéterminées X et Y sur $\mathbf{C}$, soit $B = A[Y/X]$ le sous-anneau du corps des fractions rationnelles $\mathbf{C}(X, Y)$ engendré par A et Y/X.

Montrer que l'unique homomorphisme d'anneaux de $\mathbf{C}[T, U]$ dans B qui applique T sur X et U sur Y/X est un isomorphisme. En déduire que $A^\times = B^\times = \mathbf{C}^\times$, puis que B n'est pas un localisé de A.

EXERCICE 4

Soit K un corps et soit $\varphi : K[U, V] \to K[X]$ l'homomorphisme d'anneaux défini par les égalités $\varphi(U) = X^3$, $\varphi(V) = -X^2$ et $\varphi(a) = a$ pour tout a dans K.

1 Quels sont les noyau et image de φ ? Soit A l'image de φ.

2 Montrer que A est intègre et que son corps des fractions est isomorphe à $K(X)$.

3 Montrer que l'anneau A n'est pas principal.

EXERCICE 5

Soit A un anneau (commutatif) et soit S une partie multiplicative de A qui ne contient pas 0.

1 Si A est principal, montrer que $S^{-1}A$ est un anneau principal.

2 La réciproque est-elle vraie ?

EXERCICE 6

Soit B l'ensemble des fractions rationnelles à coefficients réels de la forme $P/(X^2+1)^n$, où $P \in \mathbf{R}[X]$ est un polynôme, $n \in \mathbf{N}$. Soit A la partie de B formée de ces fractions $P/(X^2+1)^n$ où $n \geq 1$ et où P est de degré $\leq 2n$.

1 Montrer que A et B sont des sous-anneaux de $\mathbf{R}(X)$.

2 Quels sont leurs éléments inversibles ?

3 Montrer que B est un anneau principal. Montrer que l'idéal de A engendré par $1/(X^2+1)$ et $X/(X^2+1)$ n'est pas principal.

EXERCICE 7

Soit A un anneau commutatif, soit S une partie multiplicative de A.

1 On suppose qu'il existe s et $t \in S$ tels que S soit l'ensemble des $s^n t^m$ lorsque n et m parcourent $\mathbf{N}$. Montrer que l'homomorphisme $A[X, Y] \to S^{-1}A$, $P(X, Y) \mapsto P(1/s, 1/t)$ est surjectif

et que son noyau contient l'idéal $(1-sX, 1-tY)$ engendré par $1-sX$ et $1-tY$ dans $A[X,Y]$. En déduire un isomorphisme $A[X,Y]/(1-sX,1-tY) \simeq S^{-1}A$.

2 Plus généralement, soit $\langle 1-sX_s\rangle_{s\in S}$ l'idéal de l'anneau de polynômes (en une infinité de variables) $A[(X_s)_{s\in S}]$ engendré par les polynômes $1-sX_s$, lorsque s parcourt S. Alors, l'homomorphisme canonique

$$A[(X_s)_{s\in S}] \to S^{-1}A, \quad P \mapsto P((1/s)_s)$$

induit un isomorphisme

$$A[(X_s)_{s\in S}]/\langle 1-sX_s\rangle_{s\in S} \simeq S^{-1}A.$$

EXERCICE 8

Soit A un anneau commutatif et soit S une partie multiplicative de A ne contenant pas 0. On note $\mathfrak{r}(A)$ l'ensemble des éléments nilpotents de A ; on dit que A est *réduit* si $\mathfrak{r}(A) = 0$.

1 Si A est intègre, montrer que $S^{-1}A$ est intègre.

2 Si A est réduit, montrer que $S^{-1}A$ est réduit.

3 On note $f : A \to S^{-1}A$ l'homomorphisme naturel $a \mapsto a/1$. Plus généralement, montrer que $\mathfrak{r}(S^{-1}A)$ est l'idéal engendré par l'image de $\mathfrak{r}(A)$ dans $S^{-1}A$.

EXERCICE 9

Soit A un anneau et soit S une partie multiplicative de A formée d'éléments simplifiables.

On dit qu'un anneau A_S est un anneau de fractions à droite pour S s'il existe un homomorphisme injectif $i : A \to A_S$ vérifiant les conditions suivantes :

(i) pour tout $s \in S$, $i(s)$ est inversible dans A_S ;

(ii) tout élément de A_S est de la forme $i(a)i(s)^{-1}$ pour $a \in A$ et $s \in S$.

1 Supposons que A admette un anneau de fractions à droite pour S. Montrer que pour tout $a \in A$ et tout $s \in S$, il existe $a' \in A$ et $s' \in S$ tels que $as' = sa'$ (condition de Ore).

2 On suppose inversement que cette condition est satisfaite. On définit une relation $\sim$ sur $A \times S$ par « $(a,s) \sim (b,t)$ si et seulement s'il existe c et $d \in A$ et $u \in S$ tels que $u = sc = td$ et $ac = bd$. » Montrer qu'il existe, sur l'ensemble quotient A_S, une unique structure d'anneau tel que l'application i qui à $a \in A$ associe la classe de $(a,1)$ soit un homomorphisme et tel que tout $s \in S$ soit inversible dans A_S, d'inverse la classe de $(1,s)$. En déduire que A_S est un anneau de fractions à droite pour S.

3 Soit I un ensemble de cardinal au moins 2, soit K un corps commutatif et soit $A = K\{I\}$ l'algèbre du monoïde des mots sur I. Montrer que A n'admet pas de corps des fractions à droite.

EXERCICE 10

1 Soit A un anneau commutatif, soit t un élément de A et soit $S = \{1, t, t^2, \ldots\}$ la partie multiplicative engendrée par t. On note A_t l'anneau de fractions $S^{-1}A$. Montrer que les propriétés suivantes sont équivalentes :

(1) Le morphisme canonique $i : A \to A_t$ est surjectif ;

(2) la suite décroissante d'idéaux $(t^nA)_n$ est stationnaire ;

(3) pour n assez grand, l'idéal t^nA est engendré par un idempotent.

(*Pour voir que* (2) *implique* (3), *montrer par récurrence sur k qu'une relation de la forme* $t^n = t^{n+1}a$ *implique* $t^n = t^{n+k}a^k$, *puis que* t^na^n *est un idempotent.*)

2 Soit S une partie multiplicative de A formée d'éléments s tels que les morphismes $A \to A_s$ soient surjectifs. Montrer que le morphisme $A \to S^{-1}A$ est surjectif.

3 Soit A un anneau qui est fini, ou qui est un espace vectoriel de dimension finie sur un sous-corps (ou plus généralement, un anneau *artinien*). Montrer que la condition (2) est vérifiée pour tout élément t de A.

EXERCICE 11

Soit a et b des entiers ≥ 1.

1 Montrer qu'il existe des entiers m et n tels que m soit premier à b, chaque diviseur premier de n divise b, et tels que $a = mn$. (Attention, n *n'est pas* le pgcd de a et b).

2 Montrer que l'anneau $(\mathbf{Z}/a\mathbf{Z})_b$ est isomorphe à $\mathbf{Z}/n\mathbf{Z}$. On exhibera un homomorphisme de $\mathbf{Z}/n\mathbf{Z}$ sur $(\mathbf{Z}/a\mathbf{Z})_b$ dont on montrera que c'est un isomorphisme.

EXERCICE 12

1 Montrer que l'anneau $\mathbf{Z}[i]$ est isomorphe à l'anneau $\mathbf{Z}[X]/(X^2+1)$.

2 Soit a un entier. En considérant $\mathbf{Z}[i]/(a+i)$ comme un quotient de $\mathbf{Z}[X]$, définir un isomorphisme

$$\mathbf{Z}[i]/(a+i) \xrightarrow{\sim} \mathbf{Z}/(a^2+1)\mathbf{Z}.$$

3 Plus généralement, soit a et b deux entiers premiers entre eux. Montrer que l'image de b dans $\mathbf{Z}[i]/(a+ib)$ est inversible. Exprimer cet anneau comme un quotient de $\mathbf{Z}_b[X]$ puis définir un isomorphisme

$$\mathbf{Z}[i]/(a+ib) \xrightarrow{\sim} \mathbf{Z}/(a^2+b^2)\mathbf{Z}.$$

(*Noter que si* $1 = au + bv$, *alors* $1 = (a+bi)u + b(v-ui)$.)

B. IDÉAUX MAXIMAUX, IDÉAUX PREMIERS

EXERCICE 13

Montrer, en exhibant à chaque fois un isomorphisme explicite, les isomorphies suivantes :

1 $A[X] \simeq A[X,Y]/(X^2+Y+1)$, A étant un anneau commutatif ;

2 $K[X,Y]/(XY^2+1, X^2+Y+1)$, K étant un corps ;

3 $\mathbf{F}_p[X]/(X^2+1) \simeq \mathbf{Z}[X]/(X^3+X+p, X^2+1)$;

4 $\mathbf{R}[X,Y]/(X^2+1, Y^2-1) \simeq \mathbf{C}\times\mathbf{C}$.

EXERCICE 14

Pour chacune des parties Z de $\mathbf{C}^2$ suivantes, déterminer un système de générateurs raisonnable de l'idéal des polynômes de $\mathbf{R}[X,Y]$ s'annulant identiquement sur Z. Préciser aussi parmi ces idéaux ceux qui sont premiers, resp. maximaux.

1 $Z_1 = \{(0,0)\}$;

2 $Z_2 = \{(0,0),(0,1)\}$;

3 $Z_3 = \{(x,x)\,;\, x\in\mathbf{R}\}$;

4 $Z_4 = \{(x,x^2)\,;\, x\in\mathbf{C}\}$;

5 $Z_5 = \{(x,x^2)\,;\, x\in\mathbf{N}\}$;

6 $Z_6 = \{(x^2,x^3)\,;\, x\in\mathbf{R}\}$;

7 $Z_7 = \{(x,|x|)\,;\, x\in\mathbf{R}\}$;

8 $Z_8 = \{(x,\sin(x))\,;\, x\in\mathbf{R}\}$.

EXERCICE 15

1 L'ensemble des fonctions à support compact, l'ensemble des fonctions qui s'annulent pour tout entier assez grand, sont des idéaux stricts de l'anneau des fonctions continues sur $\mathbf{R}$. Ils ne sont contenus dans aucun idéal $\mathfrak{m}_x$.

2 Soit A l'anneau des fonctions holomorphes sur un voisinage du disque unité fermé. Montrer que tout idéal de A est engendré par un polynôme $P\in\mathbf{C}[z]$ dont les racines sont de modules ≤ 1. Les idéaux maximaux de A sont les idéaux $(z-a)$, pour $a\in\mathbf{C}$ tel que $|a|\leq 1$.

3 Soit K une partie compacte et connexe de $\mathbf{C}$ et soit $\mathscr{H}$ l'anneau des fonctions holomorphes sur K (c'est-à-dire sur un voisinage ouvert de K). Montrer que l'anneau $\mathscr{H}$ est intègre et que ses idéaux sont principaux (on dit que $\mathscr{H}$ est un anneau principal).

EXERCICE 16

Soit A un anneau non nul et soit $\mathfrak{m}$ l'ensemble des éléments non inversibles de A. On suppose que $\mathfrak{m}$ est un sous-groupe abélien de A.

1 Montrer que pour tout $a\in A$, l'un des éléments a ou $1-a$ est inversible.

2 Montrer que $\mathfrak{m}$ est un idéal bilatère de A.

3 Montrer que $\mathfrak{m}$ est l'unique idéal à gauche maximal de A. (On dit qu'un tel anneau est *local*.)

4 Inversement, si A est un anneau qui possède un unique idéal à gauche maximal, montrer que cet idéal est égal à $\mathfrak{m}$.

EXERCICE 17

Soit A un anneau commutatif local (voir l'exercice 16). Soit I et J deux idéaux de A et $a\in A$ un élément non diviseur de 0 tel que $IJ=(a)$.

1 Montrer qu'il existe $x\in I$ et $y\in J$ tels que $xy=a$. Justifier que x et y ne sont pas diviseurs de 0.

2 En déduire que $I=(x)$ et $J=(y)$.

EXERCICE 18

Soit A l'anneau produit des corps $\mathbf{Z}/p\mathbf{Z}$, pour p parcourant l'ensemble des nombres premiers. Soit I l'ensemble des familles $(a_p)\in A$ où $a_p=0$ pour presque tout nombre premier p. Notons B l'anneau A/I.

1 Soit $\mathfrak{m}$ un idéal maximal de A qui ne contient pas I. Montrer qu'il existe un nombre premier q tel que $\mathfrak{m}$ soit l'ensemble des familles (a_p), avec $a_q = 0$. Déterminer l'anneau quotient $A/\mathfrak{m}$.

2 Soit p un nombre premier. Montrer que $pB = B$.

3 Montrer que l'anneau B possède une unique structure de $\mathbf{Q}$-algèbre.

4 Pour tout idéal maximal $\mathfrak{m}$ de A contenant I, le corps $A/\mathfrak{m}$ est de caractéristique zéro.

EXERCICE 19

Si I est un idéal de $\mathbf{C}[X_1,\dots,X_n]$, on note $\mathscr{V}(I)$ l'ensemble des $(x_1,\dots,x_n) \in \mathbf{C}^n$ tels que $P(x_1,\dots,x_n) = 0$ pour tout $P \in I$. Si Z est une partie de $\mathbf{C}^n$, on note $\mathscr{I}(Z)$ l'ensemble des $P \in \mathbf{C}[X_1,\dots,X_n]$ tels que $P(x) = 0$ pour tout $x \in Z$.

1 Si $I \subset I'$, $\mathscr{V}(I') \subset \mathscr{V}(I)$. En outre, $I \subset \mathscr{I}(\mathscr{V}(I))$.

2 Si $Z \subset Z'$, $\mathscr{I}(Z') \subset \mathscr{I}(Z)$. Montrer aussi que $Z \subset \mathscr{V}(\mathscr{I}(Z))$.

3 Pour que $\mathscr{V}(I)$ soit vide, il faut et il suffit que I soit égal à $\mathbf{C}[X_1,\dots,X_n]$.

4 Soit $P \in \mathscr{I}(\mathscr{V}(I))$ et soit J l'idéal de $\mathbf{C}[X_1,\dots,X_n,T]$ engendré par I et le polynôme $1 - TP(X_1,\dots,X_n)$. Montrer que $\mathscr{V}(J) = 0$. En déduire qu'il existe des polynômes $P_i \in I$, Q et $Q_i \in \mathbf{C}[X_1,\dots,X_n,T]$ tels que $1 = (1-TP)Q + \sum Q_i P_i$. Montrer alors qu'il existe m tel que $P^m \in I$. (*Poser d'abord formellement* $T = 1/P$ *puis chasser les dénominateurs.*)

5 Montrer que $\mathscr{I}(\mathscr{V}(I))$ est égal à $\sqrt{I}$ (l'ensemble des éléments de $\mathbf{C}[X_1,\dots,X_n]$ dont une puissance appartient à I).

EXERCICE 20

1 Soit I et J des idéaux d'un anneau commutatif A et soit P un idéal premier de A tel que $IJ \subset P$. Montrer que l'on a $I \subset P$ ou $J \subset P$.

2 Soit $f\colon A \to B$ un homomorphisme d'anneaux. Si $I \subset B$ est un idéal premier de B, montrer que $f^{-1}(I)$ est un idéal premier de B.

3 Soit S une partie multiplicative de A et soit $f\colon A \to S^{-1}A$ l'homomorphisme canonique. Montrer que l'application $I \mapsto f^{-1}(I)$ induit une bijection de l'ensemble des idéaux premiers de $S^{-1}A$ sur l'ensemble des idéaux premiers de A qui sont disjoints de S.

EXERCICE 21

Soit k un corps. Soit A l'anneau $k^{\mathbf{N}}$ et N l'ensemble $k^{(\mathbf{N})}$ des suites $(x_n) \in A$ telles que $x_n = 0$ pour n assez grand.

1 Montrer que N est un idéal de A. Justifier qu'il existe un idéal maximal $\mathfrak{m}$ de A qui contient N. On pose alors $K = A/\mathfrak{m}$.

2 Montrer que K est une extension de k, de cardinal non dénombrable.

3 Si k est algébriquement clos, montrer qu'il en est de même de K.

4 Soit I un idéal de $k[X_1,\dots,X_n]$ et soit J le sous-K-espace vectoriel de $K[X_1,\dots,X_n]$ engendré par les éléments de I. Si $I \neq (1)$, montrer que $J \neq (1)$.

5 Utiliser le cas du théorème des zéros de Hilbert prouvé dans le cours et la construction précédente pour en déduire le cas général.

C. ANNEAUX PRINCIPAUX ET EUCLIDIENS

EXERCICE 22

On pose $A = \mathbf{C}[X,Y]/(XY-1)$. On note x l'image de X dans A.

1 Montrer que x est inversible dans 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 est dans $\mathbf{Z}$ et où P est un polynôme à coefficients dans $\mathbf{C}$ dont le terme constant est non nul. On note $e(a)$ le degré de P.

2 Soit a et b deux éléments de A, avec $b \neq 0$. Montrer qu'il existe des éléments q et r dans A tels que $a = bq + r$ avec $r = 0$ ou bien $e(r) < e(b)$.

3 En déduire que A est principal.

EXERCICE 23

1 Montrer que l'idéal $(2, X)$ de $\mathbf{Z}[X]$ n'est pas principal.

2 Soit A un anneau commutatif tel que l'anneau $A[X]$ soit principal. Montrer que A est un corps.

EXERCICE 24

Soit A l'ensemble des nombres réels de la forme $a + b\sqrt{2}$, avec a et $b \in \mathbf{Z}$. Soit K l'ensemble des nombres réels de la forme $a + b\sqrt{2}$ avec a et $b \in \mathbf{Q}$.

1 Montrer que K est un sous-corps de $\mathbf{R}$ et que A est un sous-anneau de K. Montrer aussi que $(1, \sqrt{2})$ est une base de A comme $\mathbf{Z}$-module et une base de K comme $\mathbf{Q}$-espace vectoriel.

2 Pour $x = a + b\sqrt{2} \in K$, on pose $\delta(x) = \left|a^2 - 2b^2\right|$. Montrer que $\delta(xy) = \delta(x)\delta(y)$ pour tous x, $y \in K$.

3 Pour $x = a + b\sqrt{2} \in K$, on pose $\{x\} = \{a\} + \{b\}\sqrt{2}$, où $\{t\}$ désigne le nombre entier le plus proche d'un nombre réel t, choisi inférieur à t en cas de litige. Montrer que $\delta(x - \{x\}) \leq \frac{1}{2}$.

4 Montrer que A est euclidien pour δ.

EXERCICE 25

Soit K l'ensemble des nombres complexes de la forme $a + b\frac{1+i\sqrt{3}}{2}$, où a et $b \in \mathbf{Q}$, et soit A l'ensemble des éléments de K où a et $b \in \mathbf{Z}$.

1 Montrer que K est un sous-corps de $\mathbf{C}$ et que A est un sous-anneau de K.

2 Montrer que A est un anneau euclidien pour l'application $z \mapsto |z|^2$.

EXERCICE 26

Soit A un anneau intègre et soit $\delta : A\backslash\{0\} \to \mathbf{N}$ une application qui vérifie la seconde propriété des jauges des anneaux euclidiens, à savoir : pour tous a et b dans A, $b \neq 0$, il existe q et $r \in A$ tels que $a = bq + r$ et tels que $r = 0$ ou $\delta(r) < \delta(b)$. Pour $a \in A$, on pose $\delta'(a) = \min_{b \neq 0} \delta(ab)$.

Montrer que δ' est une jauge sur A et donc que A est un anneau euclidien.

EXERCICE 27

Soit A un anneau euclidien, de jauge δ.

1 Soit $a \in A$ un élément non nul, non inversible de jauge minimale. Montrer que pour tout $x \in A$ qui n'est pas multiple de a, il existe un élément inversible $u \in A$ tel que $1 - ux$ soit multiple de a.

2 Soit n le nombre d'éléments inversibles de A. Montrer qu'il existe un idéal maximal $\mathfrak{m} \subset A$ tel que le cardinal de $A/\mathfrak{m}$ soit inférieur ou égal à $n+1$.

EXERCICE 28

Soit A le sous-anneau de $\mathbf{C}$ engendré par $\varepsilon = (1 + i\sqrt{19})/2$.

1 Montrer que $\varepsilon^2 = \varepsilon - 5$. En déduire que A est un $\mathbf{Z}$-module libre de base $(1, \varepsilon)$.

2 Montrer que pour tout $a \in A$, $|a|^2$ est entier. En déduire qu'un élément $a \in A$ est inversible si et seulement si $|a|^2 = 1$. En déduire que $A^\times = \{-1, +1\}$.

3 Soit $\mathfrak{m}$ un idéal maximal de A. Montrer qu'il existe un nombre premier p tel que $p \in \mathfrak{m}$. Montrer que $A/\mathfrak{m}$ a pour cardinal p^2 si $P = X^2 - X + 5$ est irréductible dans $\mathbf{Z}/p\mathbf{Z}$, et pour cardinal p sinon.

4 Montrer que le polynôme $X^2 - X + 5$ est irréductible dans les corps $\mathbf{Z}/2\mathbf{Z}$ et $\mathbf{Z}/3\mathbf{Z}$; en déduire que le cardinal de $A/\mathfrak{m}$ est au moins égal à 4.

5 Montrer que A n'est pas un anneau euclidien.

D. ANNEAUX FACTORIELS

EXERCICE 29

Soit A l'ensemble des nombres complexes de la forme $a+bi\sqrt{5}$, où a et $b \in \mathbf{Z}$.

1 Montrer que A est un sous-anneau de $\mathbf{C}$.

2 Montrer que les seuls éléments inversibles de A sont 1 et -1.

3 Montrer que 2, 3, $1+i\sqrt{5}$ et $1-i\sqrt{5}$ sont irréductibles dans A.

4 En observant que $2\cdot 3 = (1+i\sqrt{5})(1-i\sqrt{5})$, montrer que A n'est pas un anneau principal.

EXERCICE 30

Soit A un anneau principal.

1 Soit a un élément non nul de A. Démontrer que $A/(a)$ est de longueur finie ; calculer sa longueur en termes de la décomposition en facteurs irréductibles de a.

2 Utiliser le théorème de Jordan-Hölder pour donner une seconde démonstration de l'unicité de la décomposition en facteurs irréductibles.

EXERCICE 31

Cet exercice est la base de l'algorithme de Berlekamp pour factoriser des polynômes sur des corps finis.

Soit P un polynôme non constant à coefficients dans le corps fini $\mathbf{F}_p$. On suppose que P est *séparable* c'est-à-dire que P et P' sont premiers entre eux.

Notons R_P l'anneau $\mathbf{F}_p[X]/(P)$. Soit $P = \prod_{i=1}^{r} P_i$ la factorisation de P en polynômes irréductibles de $\mathbf{F}_p[X]$. Notons $n_i = \deg P_i$.

1 Montrer que l'anneau R_{P_i} est isomorphe au corps fini $\mathbf{F}_{p^{n_i}}$.

2 Si $A \in R_P$, on désigne par $\rho_i(A)$ le reste de la division euclidienne de A par P_i. Montrer que l'application $A \mapsto (\rho_1(A), \ldots, \rho_r(A))$ définit un isomorphisme d'anneaux $R_P \simeq \prod_{i=1}^{r} R_{P_i}$.

3 Si $A \in R_P$, posons $t(A) = A^p - A$. Montrer que t est un endomorphisme $\mathbf{F}_p$-linéaire de R_P (vu comme un $\mathbf{F}_p$-espace vectoriel) et qu'il correspond, par les isomorphismes précédents, à l'application

$$\prod_{i=1}^{r} \mathbf{F}_{p^{n_i}} \to \prod_{i=1}^{r} \mathbf{F}_{p^{n_i}}, \qquad (a_1, \ldots, a_r) \mapsto (a_1^p - a_1, \ldots, a_r^p - a_r).$$

4 Montrer que le noyau de t est un sous-espace vectoriel de R_P de dimension r.

5 Soit a un élément du noyau de t. Montrer qu'il existe un polynôme unitaire $Q \in \mathbf{F}_p[X]$ de degré minimal tel que $Q(a) = 0$. Montrer que le polynôme Q est séparable et scindé sur $\mathbf{F}_p$.

6 (*suite*) Si $a \notin \mathbf{F}_p$, montrer que Q n'est pas irréductible. D'une factorisation partielle $Q = Q_1 Q_2$, montrer comment obtenir une factorisation partielle non triviale de P.

EXERCICE 32

Soit p un nombre premier et considérons le polynôme $P = X^n + X + p$, où $n \geq 2$.

1 Supposons $p \neq 2$. Montrer que toute racine complexe de P vérifie $|z| > 1$.

2 Toujours pour $p \neq 2$, montrer que P est irréductible dans $\mathbf{Z}[X]$.

3 Supposons maintenant $p = 2$. Si n est pair, montrer que P est irréductible dans $\mathbf{Z}[X]$. Si n est impair, montrer que $X+1$ divise P et que $P/(X+1)$ est irréductible dans $\mathbf{Z}[X]$.

4 Plus généralement, tout polynôme $P = a_n X^n + \cdots + a_1 X + a_0$ tel que $|a_0|$ soit un nombre premier strictement supérieur à $|a_1| + \cdots + |a_n|$ est irréductible.

EXERCICE 33

Soit n un entier ≥ 2 et S le polynôme $X^n - X - 1$. Le but du problème est de montrer, en suivant Selmer (*Math. Scand.* **4** (1956), p. 287–302) que S est irréductible dans $\mathbf{Z}[X]$.

1 Montrer que S a n racines distinctes dans $\mathbf{C}$.

2 Pour tout polynôme $P \in \mathbf{Q}[X]$ tel que $P(0) \neq 0$, on pose

$$\varphi(P) = \sum_{j=1}^{m} \left(z_j - \frac{1}{z_j}\right),$$

où $z_1, \ldots, z_m$ sont les racines complexes de P, répétées suivant leur multiplicité.

Calculer $\varphi(P)$ en fonction des coefficients de P. Calculer $\varphi(S)$.

Si P et Q sont deux polynômes de $\mathbf{Q}[X]$ tels que $P(0)Q(0) \neq 0$, montrer que $\varphi(PQ) = \varphi(P) + \varphi(Q)$.

3 Si z est une racine de S, montrer l'inégalité

$$2\Re\big(z - \frac{1}{z}\big) > \frac{1}{|z|^2} - 1.$$

(Poser $z = re^{i\theta}$ et évaluer $\cos(\theta)$ en fonction de r.)

4 Si $x_1, \ldots, x_m$ sont des nombres réels strictement positifs tels que $\prod_{j=1}^{m} x_j = 1$. Montrer l'inégalité $\sum_{j=1}^{m} x_j \geq m$.

5 Soit P et Q deux polynômes de $\mathbf{Z}[X]$ de degrés non nuls tels que $S = PQ$. Montrer que $|P(0)| = 1$ puis que $\varphi(P)$ est un entier strictement positif. En déduire une contradiction, et donc que S est un polynôme irréductible dans $\mathbf{Z}[X]$.

EXERCICE 34. — Critère d'irréductibilité d'Eiseinstein

Soit A un anneau factoriel et K son corps des fractions. Soit

$$f(X) = \sum_{0 \leq k \leq n} a_k X^k$$

un polynôme de degré $n \geq 1$ à coefficients dans A. Soit p un élément irréductible de A. On suppose que p ne divise pas a_n, que p divise a_k si $0 \leq k < n$ et que p^2 ne divise pas a_0. Montrer que f est irréductible dans $K[X]$.

EXERCICE 35

Soit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ un polynôme unitaire dans $\mathbf{Z}[X]$ tel que $a_0 \neq 0$ et

$$|a_{n-1}| > 1 + |a_{n-2}| + \cdots + |a_0|.$$

1 À l'aide du théorème de Rouché en théorie des fonctions d'une variable complexe, montrer que P a exactement une racine complexe de valeur absolue ≥ 1.

2 Montrer que P est irréductible dans $\mathbf{Z}[X]$ (*théorème de Perron*).

EXERCICE 36

On considère l'anneau $\mathbf{C}[X, Y]$ des polynômes à coefficients dans $\mathbf{C}$ en les indéterminées X et Y. Soit I l'idéal de $\mathbf{C}[X, Y]$ engendré par l'élément $Y^2 - X^3 + X$ et A l'anneau $\mathbf{C}[X, Y]/I$. On note x et y les classes de X et Y dans A.

Le but de l'exercice est de montrer que A n'est pas un anneau factoriel.

1 Montrer que A est intègre.

2 Montrer que l'homomorphisme canonique $\mathbf{C}[T] \to A$ tel que $T \mapsto x$ est injectif. En déduire que le sous-anneau $\mathbf{C}[x]$ de A engendré par $\mathbf{C}$ et x est isomorphe à l'anneau des polynômes $\mathbf{C}[T]$. Le degré d'un élément de $\mathbf{C}[x]$ sera par définition le degré du polynôme de $\mathbf{C}[T]$ dont il est l'antécédent.

3 Soit a un élément de A. Montrer qu'il existe des éléments p et q uniques dans $\mathbf{C}[x]$ tels que l'on ait $a = p + qy$.

4 Montrer que l'application $\sigma\colon A \to A$ définie par $\sigma(p + qy) = p - qy$ est un automorphisme de A qui fixe les éléments de $\mathbf{C}[x]$.

5 Pour tout a dans A, on pose $N(a) = a\sigma(a)$. Vérifier que pour tout a, $N(a)$ appartient à $\mathbf{C}[x]$, que $N(1) = 1$ et que le degré de $N(a)$ est différent de 1. Montrer que pour tous a et b dans A, on a $N(ab) = N(a)N(b)$.

6 Déduire des questions 2, 3 et 5 que $\mathbf{C} \setminus \{0\}$ est l'ensemble des unités de A.

7 Montrer que x, y, $1-x$ et $1+x$ sont irréductibles dans A.

8 Montrer que A n'est pas factoriel.

EXERCICE 37

Si $n \geq 1$, soit $\Phi_n \in \mathbf{C}[X]$ l'unique polynôme unitaire dont les racines sont simples, égales aux racines primitives n^{e} de l'unité dans $\mathbf{C}$.

1 Montrer que $\prod_{d|n} \Phi_d = X^n - 1$. En déduire par récurrence que pour tout n, $\Phi_n \in \mathbf{Z}[X]$.

2 Si p est un nombre premier, calculer $\Phi_p(X)$. Montrer qu'il existe des entiers $a_1, \ldots, a_{p-1}$ tels que $\Phi_p(1 + X) = X^{p-1} + pa_1X^{p-2} + \cdots + pa_{p-1}$, avec $a_{p-1} = 1$. À l'aide du critère d'Eisenstein de l'exercice 34, en déduire que Φ_p est irréductible dans $\mathbf{Q}[X]$.

3 Soit n un entier, $n \geq 2$ et soit ζ une racine primitive n^{e} de l'unité. On va montrer que Φ_n est irréductible dans $\mathbf{Q}[X]$. Soit P le polynôme minimal de ζ. Montrer que $P \in \mathbf{Z}[X]$ et qu'il divise Φ_n dans $\mathbf{Z}[X]$.

Soit p un nombre premier ne divisant pas n. Montrer qu'il existe $b \in \mathbf{Z}[\zeta]$ tel que $P(\zeta^p) = pb$.

4 Montrer que ζ^p est une racine primitive n^{e} de l'unité. Si $P(\zeta^p) \neq 0$, montrer en dérivant le polynôme $X^n - 1$ que $n\zeta^{p(n-1)} \in p\mathbf{Z}[\zeta]$. En déduire une contradiction et donc que pour tout nombre premier p premier à n, $P(\zeta^p) = 0$.

5 Montrer que Φ_n est irréductible dans $\mathbf{Q}[X]$.

EXERCICE 38

Soit K un corps et soit $E = K(X)$ le corps des fractions rationnelles à coefficients dans K.

1 Montrer qu'il existe deux K-automorphismes de E, uniques, α et β tels que $\alpha(X) = 1/X$ et $\alpha(X) = 1 - X$. Montrer que le sous-groupe G de $\mathrm{Gal}(E/K)$ engendré par α et β est fini, isomorphe au groupe symétrique $\mathfrak{S}_3$.

2 Soit F le corps E^G formé des fractions rationnelles $P \in K(X)$ telles que $\alpha(P) = \beta(P) = P$. Montrer que F contient la fraction

$$f(X) = \frac{(X^2 - X + 1)^3}{X^2(X-1)^2}.$$

3 Montrer que l'extension $K(f) \subset E$ est finie de degré 6. En déduire que $F = K(f)$.

EXERCICE 39

Soit $K \subset \mathbf{C}(T)$ un sous-corps contenant $\mathbf{C}$ mais distinct de $\mathbf{C}$.

1 Montrer que l'extension $K \subset \mathbf{C}(T)$ est algébrique, finie.

2 On note $n = [\mathbf{C}(T) : K]$ son degré. Montrer que le polynôme minimal de T sur K est de la forme

$$f(X) = X^n + k_1 X^{n-1} + \cdots + k_n$$

et qu'il existe $j \in \{1; \ldots; n\}$ tel que $k_j \notin \mathbf{C}$.

3 On fixe un tel entier j et on note $u = k_j = g/h$ où $g, h \in \mathbf{C}[T]$ sont deux polynômes premiers entre eux. Soit $m = \max(\deg g, \deg h)$. Montrer que $m \geq n$. Montrer aussi qu'il existe $q \in K[X]$ tel que $g(X) - uh(X) = q(X)f(X)$.

4 Montrer qu'il existe des polynômes $c_0, \ldots, c_n \in \mathbf{C}[T]$ premiers entre eux tels que pour tout i, $c_i/c_0 = k_i$. On pose $f(X,T) = c_0(T)X^n + \cdots + c_n(T)$. Montrer que $f(X,T)$ est irréductible dans $\mathbf{C}[X,T]$.

5 Montrer qu'il existe $q \in \mathbf{C}[X,T]$ tel que

$$g(X)h(T) - g(T)h(X) = q(X,T)f(X,T).$$

En déduire que $m = n$ et donc que $K = \mathbf{C}(u)$ (*théorème de Lüroth*).

EXERCICE 40

Soit A un anneau commutatif.

1 Soit P et $Q \in A[X]$ des polynômes. On suppose que les coefficients de P, resp. ceux de Q, engendrent l'idéal (1). Montrer qu'il en est de même des coefficients de PQ. (*Adapter la démonstration du lemme de Gauss : observer que l'hypothèse entraîne que modulo chaque idéal maximal de A, P et Q sont non nuls.*)

2 Montrer qu'il existe des polynômes $W_i \in \mathbf{Z}[P_0, \ldots, P_n, Q_0, \ldots, Q_n, U_0, \ldots, U_n, V_0, \ldots, V_n]$ (pour $0 \leq i \leq 2n$) tels que si $P = \sum p_i X^i$, $Q = \sum q_i X^i$ sont des polynômes de degrés au plus n, $1 = \sum p_i u_i$ et $1 = \sum q_i v_i$ des relations de Bézout pour les coefficients de P et de Q, alors, notant $PQ = \sum r_i X^i$, on a la relation de Bézout

$$1 = \sum_{i=0}^{2n} r_i W_i(p_0, \ldots, p_n, q_0, \ldots, q_n, u_0, \ldots, u_n, v_0, \ldots, v_n)$$

pour les coefficients de PQ. (Calculer les W_i pour $n = 1$ ne semble pas une mince affaire...)

3 Pour $P \in A[X]$, notons $\mathrm{ict}(P)$ l'idéal de A engendré par les coefficients de P. La première question entraîne que $\mathrm{ict}(PQ) = A$ si $\mathrm{ict}(P) = \mathrm{ict}(Q) = A$. Lorsque A est principal, $\mathrm{ict}(P)$ est l'idéal engendré par le contenu de P et l'on a donc $\mathrm{ict}(PQ) = \mathrm{ict}(P)\,\mathrm{ict}(Q)$ d'après le lemme de Gauss. Montrer cependant que $\mathrm{ict}(PQ) \neq \mathrm{ict}(P)\,\mathrm{ict}(Q)$ en général, par exemple lorsque $A = \mathbf{C}[U,V]$, $P = UX + V$ et $Q = VX + U$.