Anneaux et corps

1 Généralités et définitions

1.1 Définition

Un ensemble A muni de deux lois + et . (appelées addition et multiplication) est un *anneau* ssi :

(i) $(A, +)$ est un groupe commutatif;

(ii) la loi . est associative et possède un élément neutre noté 1_A (ou 1 s'il n'y a pas d'ambiguïté);

(iii) . est distributive par rapport à l'addition.

Si de plus la loi . est commutative on dit que l'anneau A est *commutatif*.

Le neutre pour l'addition se note 0_A (ou 0 s'il n'y-a pas d'ambiguïté).

Exemples : $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$, $(\mathbb{Z}/n\mathbb{Z}, \overline{+}, \overline{\times})$, $F(E, A)$ ensemble des applications de E dans un anneau A muni de l'addition et de la multiplication des applications, $A[X]$ ensemble des polynômes à coefficients dans A sont des anneaux commutatifs.

$L(E)$ ensemble des endomorphismes de l'espace vectoriel E muni de l'addition et de la composition et $M_n(A)$ ensemble des matrices $n \times n$ à coefficients dans un anneau A sont des anneaux *non commutatifs*.

$P(E)$ ensemble des parties d'un ensemble E muni de la différence symétrique Δ ($A \Delta B = A \cup B - A \cap B$) et de l'intersection est un anneau commutatif appelé *anneau de Boole*.

1.2 Règles de calculs

Dans un anneau A :

$\forall\, x \in A : 0.x = x.0 = 0$;

$\forall\, (x, y) \in A \times A : x.(-y) = (-x).y = -xy$;

$\forall\, (x, y) \in A \times A$ et $\forall\, n \in \mathbb{N} : x.(ny) = (nx).y = n(x.y)$.

Formule du binôme de Newton :

Si a et b sont deux éléments permutables (i.e : $a.b = b.a$) d'un anneau A on a pout tout $n \in \mathbb{N}$:

$$(a + b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k} .$$

Démonstration : on calcule de deux façons $[0 + 0].x$. C'est égal d'une part à $0.x$. En utilisant la distributivité de l'addition sur la multiplication c'est aussi égal à $0.x + 0.x$. Donc $0.x = 0.x + 0.x$ d'où $0.x = 0$.

En considérant $[x + (-x)].y$ on montre de même que $x.(-y) = (-x).y = -x.y$.

La dernière relation se démontre d'abord pour $n \in \mathbb{N}$ par récurrence puis dans le cas général en utilisant la deuxième relation.

Formule du binôme de Newton : se démontre comme dans $\mathbb{R}$ ou $\mathbb{C}$ par récurrence sur n.

1.3 Sous-anneaux

Définition : Une partie B d'un anneau A contenant 1_A et stable pour les deux lois d'un anneau A est un *sous-anneau* de A ssi B muni des deux lois induites de celle de A est un anneau.

Caractérisation pratique

Une partie B d'un anneau $(A, +, \times)$ est un sous-anneau de A ssi :

(i) $1 \in B$;

(ii) $\forall (a, b) \in B \times B,\ x - y \in B$ et $x.y \in B$.

Remarque : avec la définition que l'on a adoptée d'un anneau la première condition ne doit pas être oubliée : par exemple $2\mathbb{Z}$ *n'est pas un sous-anneau de* $\mathbb{Z}$ car il ne contient pas 1.

Exemple : $\{a + b\sqrt{2} / a \text{ et } b \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{Q}$.

1.4 Anneaux intègres

Définitions : un élément a d'un anneau A est un *diviseur de zéro* ssi il est non nul et s'il existe $b \in A$ non nul tel que : $a.b = 0$.

Un anneau A est *intègre* ssi $A \neq \{0\}$ et si A n'a pas de diviseur de zéro, autrement dit si on a :

$a.b = 0 \Rightarrow (a = 0 \text{ ou } b = 0)$.

Exercice 1

Rechercher dans les exemples précédents les anneaux intègres.

(En particulier on a : $\mathbb{Z}/n\mathbb{Z}$ intègre $\Leftrightarrow n = 0$ ou n premier;

$A[X]$ intègre $\Leftrightarrow$ A intègre.)

1.5 Anneaux produits

Définition : si A_1 et A_2 sont deux anneaux, $A_1 \times A_2$ muni des deux lois-produits (« composantes par composantes ») est un anneau, appelé *anneau-produit* de A_1 et A_2.

On peut généraliser à un nombre quelconque d'anneaux.

Remarque : un anneau produit $A_1 \times A_2$ n'est *jamais intègre*, même si A_1 et A_2 le sont.

1.6 Morphismes d'anneaux

Définition : une application f d'un anneau A dans un anneau B est un *morphisme d'anneau* ssi :

(i) $f(1_A) = 1_B$

(ii) $\forall (x, y) \in A \times A : f(x + y) = f(x) + f(y)$

(iii) $\forall (x, y) \in A \times A : f(x.y) = f(x).f(y)$

On démontre facilement les propriétés suivantes :

Propriétés : si f est un morphisme d'anneau on a :

(i) $f(0_A) = 0_B$

(ii) Si B est un sous-anneau de A, $f(B)$ est un sous-anneau de A';

(iii) Si B' est un sous-anneau de A', $f^{-1}(B')$ est un sous-anneau de A.

1.7 Corps

1.7.1 Définitions

Définition : On appelle *corps* tout anneau non nul (i.e. $\neq \{0\}$) où tout élément non nul admet un inverse.

Si la loi . est commutative on dit qui le corps est *commutatif*.

Remarques :

on démontre que *tout corps fini est commutatif (théorème de Wedderburn).*

Un corps est intègre et donc n'a pas de diviseur de zéro.

Exercice 2

Montrer que tout anneau fini intègre est un corps.

(Pour $a \neq 0$ considérer l'application $x \mapsto a.x$ et montrer qu'elle est injective).

Exercice 3

Montrer que $\mathbb{Z}/p\mathbb{Z}$ est un corps ssi p est premier.

1.7.2 Sous-corps

Définition : Si K est un corps et si $K' \subset K$ est stable pour les lois induites, on dit que K' est un *sous-corps* de K ssi K' est un corps pour les lois induites. On dit aussi que K est une *extension* de K'.

Exercice 4

Montrer que $\{a + b\sqrt{2} / a \text{ et } b \in \mathbb{Q}\}$ est un corps.

Caractérisation pratique

$K' \subset K$ est est un sous-corps de K ssi :

(i) $1 \in K'$;

(ii) $\forall (a, b) \in K' \times K'$, $a - b$ et $a.b \in K'$;

(iii) $\forall a \in K' - \{0\}$, $a^{-1} \in K'$.

(autrement dit K' est un sous-anneau de K où tout élément non nul a un inverse dans K').

1.7.3 Corps des fractions d'un anneau intègre

Théorème et définition : Soit A un anneau intègre et commutatif. Il existe un corps K unique (à un isomorphisme près) vérifiant :

(i) K a un sous-anneau isomorphe à A;

(ii) K est minimal pour la condition (i) i.e. : si L est un corps vérifiant (i) alors L admet un sous-corps isomorphe à K.

K est appelé *corps des fractions de A* et se note Fr(A).

Exemples : $\mathbb{Q}$ = Fr($\mathbb{Z}$); $A(X)$ = Fr($A[X]$) (corps des fractions rationnelles à coefficients dans A).

2. Idéaux d'un anneau; anneaux quotients

2.1 Relations d'équivalences compatibles avec les lois d'un anneau; idéaux

Position du problème : étant donné un anneau A on cherche les relations d'équivalences $\sim$ sur A telles que les lois + et . de A « passent au quotient » i.e les relations d'équivalences compatibles avec + et . (voir exposé « groupes »). Dans ce cas $A/\sim$ muni des lois quotients est-il un anneau ?

On a vu que les relations d'équivalences compatibles avec la loi + sont celles vérifiant : $x \sim y \Leftrightarrow x - y \in I$ où I est un sous-groupe de $(A, +)$ (tout sous-groupe de A étant distingué puisque $(A, +)$ est commutatif : voir chapitre « groupes ») et alors $(A/\sim, \overline{+})$ est aussi un groupe commutatif.

La relations d'équivalences $\sim$ sera compatible avec la loi . ssi on a, pour tout a, x et y de A :

$$x \sim y \Rightarrow a.x \sim a.y \quad \text{et} \quad x.a \sim y.a$$

c'est-à-dire : $x - y \in I \Rightarrow a.(x-y) \in I$ et $(x - y).a \in I$.

On voit immédiatement que cela équivaut à :

$$\forall (a, x) \in A \times I, \ a.x \in I \text{ et } x.a \in I.$$

D'où la définition suivante :

Définition : Une partie I d'un anneau A est appelé *idéal à gauche* (respectivement *idéal à droite)* ssi :

(i) I est un sous-groupe de $(A, +)$;

(ii) $\forall a \in A, \forall x \in I : a.x \in I$ (respectivement $x.a \in I$).

Si I est un idéal à gauche et à droite à la fois de A on dit que c'est un *idéal bilatère* de A.

Remarques :

Si A est commutatif les idéaux à gauche et à droite coïncident;

$\{0\}$ et A sont des idéaux de A (dits *triviaux*);

Un idéal I de A n'est pas forcément un sous-anneau de A car il ne contient pas forcément 1. Plus précisément on a :

$$1 \in I \Leftrightarrow I = A.$$

On a donc :

Théorème : Les relations d'équivalences $\sim$ sur A compatibles avec les deux lois de A sont de la forme :

$$x \sim y \Leftrightarrow x - y \in I$$

où I est un idéal bilatère de A.

Si I est un idéal bilatère de A on peut donc définir dans l'ensemble quotient $A/\sim = A/I$ les lois quotients $\overline{+}$ et $\overline{\times}$. On peut maintenant répondre à la question du 2.1 :

2.2 Anneaux quotients

Théorème : Soit A un idéal bilatère de A. Alors A/I muni des lois quotients $\overline{+}$ et $\overline{\times}$ est un anneau.

Démonstration : immédiate.

Cet anneau $(A/I, \overline{+}, \overline{\times})$ s'appelle *anneau quotient de A par l'idéal I.*

Remarques :

Si A est commutatif, A/I aussi. Mais A peut être intègre sans que A/I le soit (par exemple $\mathbb{Z}/n\mathbb{Z}$: voir exercice 1).

Si I est un idéal à gauche de A la relation d'équivalence $\sim$ est compatible à gauche avec multiplication de A et donc on peut définir dans A/I une opération externe en posant pour tous a et x de A $a\overline{x} = \overline{ax}$. Si I est un idéal bilatère, A muni des lois internes $\overline{+}$ et $\overline{\times}$ et de cette loi externe est un A-module.

Exercice 5

Les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ $(n \in \mathbb{Z})$.

(Ainsi dans $\mathbb{Z}$ il *y*-a identité entre sous-groupe et idéal : voir « groupes »).

Exercice 6

Soit A un anneau non nul. Montrer que A est un corps ssi ses seuls idéaux à gauche sont les idéaux triviaux $\{0\}$ et A. Même question en remplaçant « idéal à gauche » par « idéal à droite ».

Exercice 7

Soit $P \in \mathbf{K}[X]$ (anneau des polynômes à coefficients dans le corps $\mathbf{K}$). Montrer que le polynôme $P(X) - X$ divise $P(P(X)) - X$ (raisonner dans $\mathbf{K}[X]/(P(X) - X)$).

Exercice 8

Soit f un morphisme d'anneaux. Montrer que Ker f est un idéal de A. Si J est un idéal de B montrer que $f^{-1}(J)$ est un idéal de A.

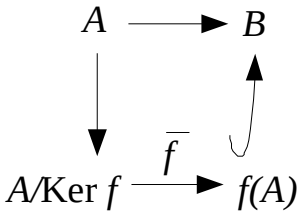
Exercice 9

Si I est un idéal de A, l'application $s : A \to A/I$ qui à x associe sa classe $\overline{x}$ (*surjection canonique*) est un morphisme d'anneaux qui induit une bijection entre les idéaux de A contenant I et les idéaux de A/I.

(**Remarque** : si I est un idéal de A, $f(I)$ n'est pas en général un idéal de B : donner un contre-exemple).

Exercice 10

Avec la notation précédente on a la *décomposition canonique de f* :



où *s* est la surjection canonique, *i* l'inclusion et $\bar{f}$ est un *isomorphisme d'anneaux*.

Exercice 11

Montrer que $\{a + b\sqrt{2} / a \text{ et } b \in \mathbb{Q}\}$ (voir exercice 4) est un anneaux isomorphe à $\mathbb{Q}[X]/(X^2-2)$ où (X^2-2) désigne l'idéal $\{(X^2-2)Q / Q \in \mathbb{Q}[X]\}$ (considérer la décomposition canonique du morphisme d'anneaux φ de $\mathbb{Q}[X]$ dans $\mathbb{Q}$ qui à P associe $P(\sqrt{2})$).

Montrer de même que $\mathbb{C}$ est isomorphe à $\mathbb{R}[X]/(X^2+1)$.

2.3 Applications : caractéristique d'un anneau

Soit *A* un anneau; l'application φ de $\mathbb{Z}$ dans *A* qui à *n* associe *n*.1 est un morphisme d'anneaux. Son noyau Ker φ est donc un idéal de $\mathbb{Z}$ (exercice 8) donc de la forme $p\mathbb{Z}$ avec $p \in \mathbb{N}$ (exercice 5). En considérant la décomposition canonique de φ (exercice 10) on obtient un isomorphisme de $\mathbb{Z}/p\mathbb{Z}$ sur $\varphi(\mathbb{Z})$.

Définition : l'entier naturel *p* ainsi défini s'appelle *caractéristique* de l'anneau *A* et se note car(*A*).

Remarques :

Si $p = 0$: alors Ker $\varphi = \{0\}$ donc φ est injective et donc $\mathbb{Z}$ est isomorphe à $\varphi(\mathbb{Z})$: *A* contient un sous-anneau isomorphe à $\mathbb{Z}$ et en particulier *A* est infini;

Si $p \neq 0$: alors Ker $\varphi = p\mathbb{Z}$ isomorphe à $\varphi(\mathbb{Z})$; *p* est le plus petit entier > 0 tel que $p.1 = 0$ et $p \in \mathbb{N}$ est caractérisé par : $\forall n \in \mathbb{N} : n.1 = 0 \Leftrightarrow n$ multiple de *p*.

Proposition : Si l'anneau *A* est *intègre* sa caractéristique est soit 0 soit un nombre premier.

En particulier la caractéristique d'un corps est donc 0 ou un nombre premier.

Démonstration : si la caractéristique de *A* n'est pas nulle $\varphi(\mathbb{Z})$ est inclus dans *A* intègre, donc $\varphi(\mathbb{Z})$ est lui-même intègre et de plus il est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Donc $\mathbb{Z}/p\mathbb{Z}$ est intègre donc *p* est premier (exercice 1).

La réciproque de la proposition est fausse (trouver des contre exemples).

Exemples : car($\mathbb{Z}/n\mathbb{Z}$) = *n*; car($\mathbb{Q}$) = car($\mathbb{R}$) = 0.

Exercice 12

Etant donné un corps *K* on appelle *sous-corps premier* de *K* le plus petit sous-corps (au sens de l'inclusion) *K'* de *K*. Montrer que si car(*K*) = 0, *K'* est isomorphe à $\mathbb{Q}$ et si car(*K*) = *p*, *K'* est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Exercice 13

Soit *K* un corps fini; montrer qu'il existe un nombre premier *p* et un entier $n > 0$ tel que Card $K = p^n$ (considérer *K* comme un espace vectoriel sur son corps premier).

Réciproquement on démontre que pour tout nombre premier *p* et tout entier $n > 0$ il existe un corps à $q = p^n$ éléments, unique à un isomorphisme près, noté $\mathbf{F}_q$.

Exercice 14

Soit *K* un corps commutatif de caractéristique $p > 0$. Montrer que l'application de *K* dans *K* qui à *x* associe x^p est un morphisme de corps (appelé *homomorphisme de Fröbenius*).

Si *K* est fini c'est un automorphisme; si $K = \mathbb{Z}/p\mathbb{Z}$ c'est l'identité (utiliser le théorème Fermat).

2.4 Idéal engendré par une partie

Définitions : Soit *X* une partie d'un anneau *A*. On appelle *idéal engendré par X* l'intersection de tous les idéaux de *A* contenant *X* : c'est donc le plus petit idéal (au sens de l'inclusion) de *A* contenant *X*.

On le note Id(*X*).

Un idéal engendré par un seul élément est appelé *idéal principal*. Si cet élément est a on note Id(a) = (a) l'idéal engendré par a. Si A est *commutatif* on a : (a) = $\{a.x / x \in A\}$.

Si (I_k) est une famille d'idéaux de A, l'idéal engendré par $\bigcup_k I_k$ est constitué des sommes finies $\sum_k x_k$ avec $x_k \in I_k$; on le note $\sum_k I_k$ et on l'appelle *somme des idéaux* I_k.

On appelle *produit* de deux idéaux I et J l'idéal engendré par les produits $x.y$ avec $x \in I$ et $y \in J$: c'est l'ensemble des sommes finie $\sum_{k=1}^{n} x_k y_k$, avec $x_k \in I$ et $y_k \in J$. On généralise immédiatement au produit un nombre fini d'idéaux.

2.5 Idéaux premiers

Définition : un idéal I d'un anneau A est *premier* ssi l'anneau quotient A/I est intègre.

Exemples : dans $\mathbb{Z}$, l'idéal (a) = $a\mathbb{Z}$ est premier ssi $a = 0$ ou a est premier (exercice 1).

Dans $\mathbb{Z}[X]$ l'idéal (X) = $\{XP(X) / P \in \mathbb{Z}[X]\}$ est premier car $\mathbb{Z}/(X)$ est isomorphe à $\mathbb{Z}$ qui est intègre (considérer le morphisme d'anneaux de $\mathbb{Z}[X]$ dans $\mathbb{Z}$ qui à $P \in \mathbb{Z}[X]$ associe $P(0)$ et le passer au quotient).

La proposition suivante donne une caractérisation des idéaux premiers d'un anneau :

Proposition : Les assertions suivantes sont équivalentes :

(i) I est un idéal premier de A;

(ii) $I \neq A$ et $\forall\ (a, b) \in A \times A$ on a : $a.b \in I \Rightarrow a \in I$ ou $b \in I$.

Démonstration :

(i) $\Rightarrow$ (ii) : soit I un idéal premier de A. A/I est différent de $\{\overline{0}\}$ donc $I \neq A$. Si $a.b \in I$ alors $\overline{a}.\overline{b} = \overline{0}$ dans A/I soit $\overline{a}$ ou $\overline{b}$ est nul car A/I est intègre donc a ou b appartient à I.

(ii) $\Rightarrow$ (i) : comme $I \neq A$, $A/I \neq \{\overline{0}\}$. D'autre part : $\overline{a}.\overline{b} = \overline{0} \Leftrightarrow a.b \in I \Rightarrow a$ ou b appartient à $I \Leftrightarrow \overline{a}$ ou $\overline{b}$ est nul et donc A/I est intègre.

Exercice 15

Soit $f : A \to B$ un homomorphisme d'anneaux et J un idéal premier de B; montrer que si $f^{-1}(J)$ est différent de A c'est un idéal premier de A.

A partir d'ici tous les anneaux considérés seront supposés commutatifs.

2.6 Idéaux maximaux

Définition : un idéal I d'un anneau A est *maximal* ssi l'anneau quotient A/I est un corps.

On a donc l'implication : I idéal maximal $\Rightarrow I$ idéal premier.

La proposition suivante donne une caractérisation des idéaux maximaux d'un anneau :

Proposition : Les assertions suivantes sont équivalentes :

(i) I est un idéal maximal de A;

(ii) $I \neq A$ et si J est un idéal de A distinct de A tel que $I \subset J$, alors $J = I$ (autrement dit I est *maximal* pour l'inclusion parmi les idéaux propres de A).

Démonstration :

(i) $\Rightarrow$ (ii) : soit I un idéal maximal de A; A/I est différent de $\{\overline{0}\}$ donc $I \neq A$. Soit J un idéal de A distinct de A tel que $I \subset J$. Si I est distinct de J considérons $x \in J - I$. On a $\overline{x} \neq \overline{0}$ donc $\overline{x}$ est inversible (car A/I est un corps) : il existe $y \in A$ tel que $\overline{x}.\overline{y} = \overline{1}$ donc il existe $z \in I$ tel que $x.y = 1 + z$ soit $1 = x.y - z$ d'où $1 \in J$ et on aurait $J = A$ contrairement à l'hypothèse. Donc $J = I$.

(ii) $\Rightarrow$ (i) : si $\overline{x}$ appartenant à $A/I - \{\overline{0}\}$ on a $x \notin I$. L'idéal $I + (x)$ engendré par I et x contient strictement I donc il est égal à A par hypothèses. Par conséquent il existe $z \in I$ et $y \in A$ tels que $1 = z + x.y$ d'où $\overline{1} = \overline{x}.\overline{y}$ et $\overline{x}$ est inversible dans A/I. Comme A/I est non nul car $A \neq I$ c'est donc un corps et I est un idéal maximal de A.

Remarque : on peut démontrer le *théorème de Krull* : tout idéal propre de A est inclus dans un idéal maximal de A (la démonstration utilise le lemme de Zorn qui équivaut à l'axiome de choix).

Exercice 16

Soit $f : A \to B$ un homomorphisme d'anneaux et J un idéal maximal de B. Que peut-on dire en général de l'idéal $f^{-1}(J)$ de A ? Et si on suppose de plus f surjective ?

(pour un contre-exemple considérer l'injection canonique de $\mathbb{Z}[X]$ dans $\mathbb{R}[X]$ et $J = (X)$).

Exercice 17 : Théorème Chinois généralisé

1°/ Montrer que si I et J sont deux idéaux de A on a : $IJ \subset I \cap J$.

2°/ On dit que deux idéaux I et J sont *étrangers* ssi $I + J = A$. Montrer que dans ce cas on a : $IJ = I \cap J$ (On notera que deux idéaux I et J sont étrangers ssi il existe $a \in I$ et $b \in J$ tels que $a + b = 1$).

Montrer que deux idéaux distincts dont l'un est maximal sont étrangers.

3°/ Montrer que si n idéaux sont étrangers deux à deux on a un isomorphisme de $A/I_1.I_2...I_n = A/I_1 \cap I_2 \cap ... \cap I_n$ dans $A/I_1 \times A/I_2 \times ... \times A/I_n$ (*théorème chinois généralisé*).

Exercice 18 : anneaux locaux

Un anneau A est *local* ssi il admet un seul idéal maximal.

Montrer qu'un anneau A est local ssi l'ensemble de ses éléments non inversibles forment un idéal de A.

(Pour la condition nécessaire utiliser le théorème de Krull).

3. Divisibilité dans les anneaux intègres; anneaux factoriels, principaux, euclidiens

3.1 Quelques définitions

3.1.1 Groupe des éléments inversibles d'un anneau

Soit A un anneau; on note A^* l'ensemble des éléments inversibles de A : il est clair que c'est un groupe pour la multiplication.

Exemples : Si A est un corps, $A^* = A - \{0\}$ et $(A[X])^* = A - \{0\}$; si A est intègre $(A[X])^* = A^*$; $\mathbb{Z}^* = \{-1; 1\}$;

$(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{x} / 0 \leq x \leq n-1$ et pgcd$(x, n) = 1\}$.

Remarquons que : $a \in A^* \Leftrightarrow (a) = A$.

3.1.2 Divisibilité

Soient a et b éléments de A; on dit que a *divise* b (on note a/b) ssi il existe $c \in A$ tel que : $b = ac$. C'est une relation de préordre dans A (i.e réflexive et transitive).

On a : $a/b \Leftrightarrow (b) \subset (a)$.

Considérons dans A la relation d'équivalence R définie par : $a\ R\ b \Leftrightarrow a/b$ et b/a.

Cela équivaut à l'existence de k et k' de A tels que: $b = ak$ et $a = bk'$; on en déduit que $b = bkk'$, soit $b.(kk' - 1) = 0$. Si A *est intègre* on a donc $k.k' = 1$ et par conséquent k et k' sont inversibles.

On a donc, si A est intègre : $a\ R\ b \Leftrightarrow \exists\ u \in A^* / a = bu$.

On dit que les éléments a et b sont *associés*. Les éléments associés jouent le même rôle pour la divisibilité, c'est-à-dire que si a et a' sont associés, ainsi que b et b' on a : $a/b \Leftrightarrow a'/b'$.

<u>Dans la suite on supposera que A est un anneau intègre.</u>

Dans A/R la relation de divisibilité est un relation d'ordre et l'application $a \mapsto (a)$ est un isomorphisme d'ensembles ordonnés de $(A/R, /)$ (ensemble quotient muni de la divisibilité) dans $(J(A), \supset)$ (ensemble des idéaux principaux de A muni de $\supset$).

3.1.3 Eléments irréductibles; théorème d'Alembert-Gauss

Un élément $p \in A$ est *irréductible* ssi :

(i) $p \notin A^*$;

(ii) $p = ab \Rightarrow a \in A^*$ ou $b \in A^*$.

(Autrement dit les seuls diviseurs de p sont les inversibles, p et les éléments associés).

La deuxième condition s'écrit aussi en termes d'idéaux : si a est non inversible on a : $(p) \subset (a) \Rightarrow (a) = (p)$, autrement dit *(p) est maximal parmi les idéaux principaux de A, distinct de A.* Si A n'est pas un corps on a donc :

p irréductible $\Leftrightarrow$ (p) est maximal parmi les idéaux principaux de A, distinct de A

<u>Exemples</u> : 0 n'est pas irréductible; un corps n'a pas d'éléments irréductibles.

Dans $\mathbb{Z}$ les irréductibles sont les nombres premiers.

Dans $\mathbb{C}[X]$ on a : P est irréductible $\Leftrightarrow$ $d°P = 1$ ce qui est équivalent au théorème suivant :

<u>Théorème d'Alembert-Gauss</u> :

Tout polynôme non constant à coefficients complexes admet au moins une racine dans $\mathbb{C}$.

<u>Démonstration</u> : Supposons que P n'admette aucune racine dans $\mathbb{C}$. Comme $\lim_{z\to+\infty}|P(z)| = +\infty$ il existe un réel $R > 0$ tel que : $|z| > R \Rightarrow |P(z)| > |P(0)|$.

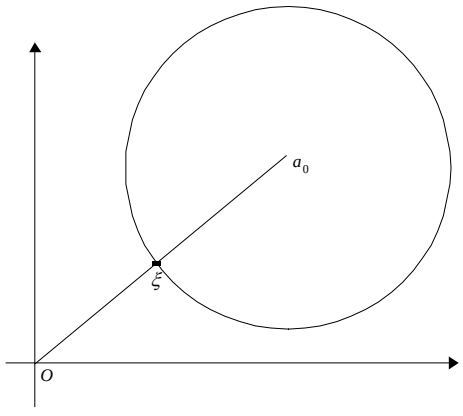
L'application $z \mapsto |P(z)|$ étant continue et le disque $D(0, R)$ de $\mathbb{C}$ étant compact car fermé borné (voir chapitre « Suites de nombres réels et complexes ») elle est bornée et atteint ses bornes. Par suite il existe z_0 de ce disque tel que $\mu = \inf_{|z|\le R}|P(z)| = |P(z_0)|$.

Pour tout z du disque on a donc $|P(z)| \ge \mu$. Si z est à l'extérieur de ce disque on a $|P(z)| > |P(0)| \ge \mu$ et ainsi $\mu = \inf_{z\in C}|P(z)|$.

Par translation on peut supposer $z_0 = 0$. On aura $P(z) = a_0 + a_p z^p + ... + a_m z^m$ avec $1 \le p \le m$, $a_p \ne 0$, $a_m \ne 0$ et $|a_0| = \mu$.

Si $a_0 = 0$ alors $P(0) = 0$ et le théorème est démontré. Supposons donc $a_0 \ne 0$.

Quand z parcourt le cercle de centre 0 et de rayon ρ, $a_0 + a_p z^p$ parcourt le cercle de centre a_0 et de rayon $|a_p|\rho^p$. Soit $\rho > 0$ tel que $|a_p|\rho^p < \mu$. Il existe $\xi = a_0 + a_p\beta^p$ ($|\beta| = \rho$) appartenant au cercle de centre a_0 et de rayon $|a_p|\rho^p$ tel que $|a_0 + a_p\beta^p| = |a_0| - |a_p|\rho^p$ (voir figure). Si $p = m$ cela s'écrit $|P(\beta)| = |a_0| - |a_p|\rho^p < |a_0| = \mu$ ce qui contredit que μ est le minimum de $|P(z)|$ sur $\mathbb{C}$.



Si $p < m$ le quotient $(a_{p+1}z^{p+1} + ... + a_m z^m)/ a_p z^p$ tend vers 0 quand z tend vers 0 et il existe $\alpha > 0$ tel que : $|z| < \alpha \Rightarrow |a_{p+1}z^{p+1} + ... + a_m z^m| < |a_p z^p| = |a_p|\rho^p$. Si ρ est choisi tel que $|\rho| < \alpha$ et β comme précédemment on a : $|P(\beta)| \le |a_0 + a_p\beta^p| + |a_{p+1}\beta^{p+1} + ... + a_m\beta^m| < |a_0| - |a_p|\rho^p + |a_p|\rho^p = |a_0| = \mu$ et on aboutit à la même contradiction.

<u>Corollaire</u> : Dans $\mathbb{R}[X]$: P est irréductible $\Leftrightarrow$ ($d°P = 1$ ou $d°P = 2$ de discriminant < 0).

3.1.4 Eléments premiers entre eux

Deux éléments a et b sont *premiers entre eux* ssi :

$\forall d \in A$: (d/a et $d/b \Rightarrow d \in A^*$).

(Autrement dit a et b n'ont pas de diviseurs communs non triviaux).

3.2 Anneaux factoriels

Définition : un anneau A est *factoriel* ssi :

(o) A est intègre;

(i) $\forall a \in A-\{0\}$, a s'écrit $up_1p_2...p_r$ avec $u \in A^*$ et $p_1, p_2, ... p_r$ irréductibles (propriété que l'on notera **(E)**);

(ii) La décomposition précédente est unique, aux inversibles près et à l'ordre près (propriété notée **(*U*)**).

Remarque : si on choisit dans l'ensemble quotient des éléments irréductibles modulo la relation d'équivalence R (voir 3.1) un système de représentants P (i.e et et un seul éléments dans chaque classe) la définition précédente s'écrit :

(o) A est intègre;

(i) $\forall a \in A-\{0\}$, a s'écrit $a = u \prod_{p\in P} p^{v_p(a)}$ avec $u \in A^*$, $v_p(a) \in \mathbb{N}$ nuls sauf un nombre fini d'entre eux (**(E)**);

(ii) La décomposition précédente est unique (**(*U*)**).

L'entier $v_p(a)$ ainsi défini s'appelle *valuation p-adique de a.*

Exercice 19

Montrer que dans un anneau factoriel pour tous a et b non nuls :

$$a/b \Leftrightarrow \forall p \in P : v_p(a) \leq v_p(b), \text{ et :}$$

$$(a) = (b) \Leftrightarrow \forall p \in P : v_p(a) = v_p(b).$$

Exemples : On verra plus loin que $\mathbb{Z}$, $\mathbf{K}[X]$, $\mathbf{K}[X_1,..., X_n]$ (où $\mathbf{K}$ est un corps), $\mathbb{Z}[i] = \{a + ib / a \in \mathbb{Z} \text{ et } b \in \mathbb{Z}\}$ (*anneau de Gauss*) sont des anneaux factoriels.

$A = \mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5} / a \in \mathbb{Z} \text{ et } b \in \mathbb{Z}\}$ est intègre et vérifie la condition (E) mais pas (*U*) puisque :

$9 = 3\times3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$ et 3, $2 + i\sqrt{5}$ et $2 - i\sqrt{5}$ sont irréductibles (voir « exercices complémentaires » III).

On s'intéresse maintenant à la condition (U) :

Proposition : Soit A un anneau intègre où la condition (E) est satisfaite. Alors les conditions suivantes sont équivalentes :

(i) A vérifie (U);

(ii) Si p est irréductible : ($p/ab \Rightarrow p/a$ ou p/b) (*lemme d'Euclide)*;

(iii) si p non nul : p irréductible $\Leftrightarrow$ l'idéal (p) est premier;

(iv) a/bc et a premier avec $b \Rightarrow a/c$ (*Théorème de Gauss*).

Démonstration :

(i) $\Rightarrow$ (ii) : comme A vérifie (U) on dispose de la valuation p-adique. Si p est irréductible et p/ab alors $v_p(p) \leq v_p(ab) = v_p(a) + v_p(b)$ soit $1 \leq v_p(a) + v_p(b)$, d'où $v_p(a) \geq 1$ ou $v_p(b) \geq 1$. On en déduit p/a ou p/b;

(ii) $\Rightarrow$ (i) : supposons qu'un élément a de $A-\{0\}$ ait deux décompositions :

$$a = u\prod_{p\in P} p^{\alpha_p} = v\prod_{p\in P} p^{\beta_p} \text{ (où les produits sont finis et } u \text{ et } v \text{ appartiennent à } A^*).$$

Supposons que pour un $p_0 \in P$ on ait $\alpha_{p_0} < \beta_{p_0}$. En simplifiant par $p_0^{\alpha_{p_0}}$ il vient $u\prod_{p\neq p_0} p^{\alpha_p} = v\prod_{p\neq p_0} p^{\beta_p}.p_0^{\beta_{p_0}-\alpha_{p_0}}$.

p_0 divise le deuxième membre donc il divise le premier. En appliquant le (ii) un nombre fini de fois on voit que p_0 divise l'un des $p \in P$ figurant au premier membre, donc p et q sont associés d'où $p = p_0$ ce qui n'est pas;

(ii) $\Rightarrow$ (iii) : sans aucune hypothèse montrons qu'on a toujours, si p est non nul : (p) premier implique p irréductible. En effet (p) $\neq A$ donc $p \notin A^*$ et si $p = ab$ alors $ab \in (p)$ donc a ou b appartient à (p) soit p divise a ou b et par suite p est irréductible.

Supposons maintenant que l'on ait (ii) et que p soit irréductible. Si $ab \in (p)$ alors p divise ab donc p divise a ou b par hypothèse soit a ou b appartient à (p). L'idéal (p) est donc premier;

(iii) $\Rightarrow$ (ii) : soit p irréductible (donc non nul) tel que p/ab. Alors $ab \in (p)$. Par hypothèse l'idéal (p) est premier donc a ou b appartient à (p) soit p divise a ou p divise b;

(i) $\Rightarrow$ (iv) : supposons que a divise bc et a premier avec b. On peut supposer a, b, c non nuls. Soit p irréductible tel que $v_p(a) \neq 0$. Comme a divise bc on a $v_p(a) \leq v_p(b) + v_p(c)$. Comme a est premier avec b on a $v_p(b) = 0$ donc $v_p(a) \leq v_p(c)$ et d'après l'exercice 19 a divise c;

(iv) $\Rightarrow$ (ii) : soit p irréductible tel que p divise ab. Si p ne divise pas a, p est premier avec a donc p divise b d'après Gauss.

Remarque : Sans l'hypothèses (E) on a toujours, si $p \neq 0$:

(p) premier $\Rightarrow$ p irréductible; (ii) $\Leftrightarrow$ (iii); (ii) $\Rightarrow$ (i); (iv) $\Rightarrow$ (i).

ppmc et pgcd : dans un anneau factoriel on a l'existence du pgcd et du ppmc de plusieurs éléments :

Théorème : Si A est un anneau factoriel et si a et b sont deux éléments de A, l'ensemble $\{a, b\}$ a un sup dans l'ensemble ordonné (A/R, /) noté ppmc(a, b) et un inf noté pgcd(a, b).

De plus, si $a = u\prod_{p\in P} p^{v_p(a)}$ et $b = v\prod_{p\in P} p^{v_p(b)}$ (u et $v \in A^*$) on a :

$$\text{ppmc}(a, b) = \prod_{p\in P} p^{\text{Max}\left(v_p(a), v_p(b)\right)} \quad \text{et} \quad \text{pgcd(a, b)} = \prod_{p\in P} p^{\text{Min}\left(v_p(a), v_p(b)\right)}.$$

Démonstration : si $a = 0$ ou $b = 0$ alors Sup$\{a, b\} = 0$. Supposons donc a et b non nuls et soit $m \in A$ tel que a/m et b/m. Pour tout p de P on a $v_p(a) \leq v_p(m)$ et $v_p(b) \leq v_p(m)$ donc Max($v_p(a)$, $v_p(b)$) $\leq v_p(m)$ soit $\mu = \prod_{p\in P} p^{\text{Max}\left(v_p(a), v_p(b)\right)}$ divise m.

Comme a et b divisent μ on en déduit que μ est la borne supérieure de a et b dans (A/R, /).

De même pour le pgcd.

Remarques :

le ppmc et le pgcd de deux éléments ne sont définis qu'à des inversibles près;

on peut généraliser à un nombre fini d'éléments;

si on travaille dans l'ensemble ordonné ($J(A)$, $\subset$) plutôt que dans (A, /) on aurait :

sup((*a*), (*b*)) = (pgcd(*a*, *b*)) et inf((*a*), (*b*)) = (ppmc(*a*, *b*));

pour tous a et b non nuls de A : ppmc(a, b).pgcd(a, b) = ab aux inversibles près;

on a $(a)\cap(b)$ = (ppmc(a, b)) *mais pas en général* : $(a) + (b)$ = (pgcd(a, b)) (voir 3.3).

Le théorème suivant donne des exemples très importants d'anneaux factoriels :

Théorème de Gauss : Si A est factoriel, $A[X]$ aussi.

Démonstration :

A étant intègre $A[X]$ aussi et $(A[X])^* = A^*$.

Si $P = a_nX^n + ... + a_0$ on pose $c(P)$ = pgcd(a_n, ... , a_0) (appelé *contenu* de P). On dira que P est *primitif* sii $c(P) = 1$. Soit **K** le corps des fractions de A.

Lemme 1 : pour tout P et Q de $A[X]$ on a : $c(PQ) = c(P)c(Q)$.

Démonstration : supposons d'abord P et A primitifs et posons $P = \sum_{k=1}^{n} a_k X^k$ et $Q = \sum_{k=1}^{m} b_k X^k$.

Supposons que $c(PQ)$ soit différent de 1 et soit p un irréductible de A divisant tous les coefficients de PQ. Posons $i_0 = \text{Max}\{k \in \mathbb{N} / p/a_0, p/a_1, \ldots, p/a_{k-1}\}$ (en convenant que $i_0 = 0$ si l'ensemble $\{k \in \mathbb{N} / p/a_0, p/a_1, \ldots, p/a_{k-1}\}$ est vide) et de même $j_0 = \text{Max}\{k \in \mathbb{N} / p/b_0, p/b_1, \ldots, p/b_{k-1}\}$ (en particulier p ne divise ni a_{i_0} ni b_{j_0}).

Le coefficient de $X^{i_0+j_0}$ de PQ est $a_{i_0}b_{j_0} + \sum_{\substack{i+j=i_0+j_0 \\ i<i_0 \text{ ou } j<j_0}} a_i b_j$. Par définition de i_0 et j_0 p divise $\sum_{\substack{i+j=i_0+j_0 \\ i<i_0 \text{ ou } j<j_0}} a_i b_j$ donc p divise $a_{i_0}b_{j_0}$. p étant irréductible p divise a_{i_0} ou p divise b_{j_0} (lemme d'Euclide) ce qui n'est pas.

Dans le cas général posons $d = c(P)$, $e = c(Q)$, $P' = P/d$ et $Q' = Q/e$. P' et Q' sont primitifs et $PQ = de.P'Q'$. On a $c(PQ) = de.c(P'Q')$ et d'après le cas précédent $c(P'Q') = 1$ d'où $c(PQ) = de$ ce qui achève la démonstration du lemme 1.

Le lemme suivant précise le irréductibles de $A[X]$.

Lemme 2 : les polynômes P irréductibles de $A[X]$ sont :

(i) les constantes p de A irréductibles dans A;

(ii) les polynômes P de degré supérieur ou égal à 1, primitifs et irréductibles dans $\mathbf{K}[X]$.

Démonstration : montrons qu'un polynôme P vérifiant (i) ou (ii) est irréductible dans $A[X]$.

si $P = p \in A$ est irréductible dans A et si $p = Q_1(X)Q_2(X)$ est prenant le degré des deux membres il vient $0 = d°(Q_1) + d°(Q_2)$ donc $d°(Q_1) = d°(Q_2) = 0$. Q_1 et Q_2 sont donc des constantes et p étant irréductible l'une d'entre elle appartient à A^* donc à $(A[X])^*$ et par suite p est irréductible dans $A[X]$.

soit P vérifiant le (ii) et supposons que $P = QR$ dans $A[X]$. Cette relation est valable dans $\mathbf{K}[X]$ par suite Q ou R est inversible dans $\mathbf{K}[X]$. Supposons par exemple que $Q = q \in A - \{0\}$. On a donc $P = qR$ d'où $c(P) = c(qR)$ soit, P étant primitif, $1 = q.c(R)$. q est donc inversible et P est irréductible dans $A[X]$.

Montrons maintenant que les polynôme vérifiant (i) et (ii) sont les seuls polynômes irréductibles de $A[X]$. Soit donc P un polynôme irréductible de $A[X]$.

Si $d°P = 0$, $P = p \in A$ et il est clair que p est irréductible dans A (car $A^* = A[X]^*$).

Si $d°P \geq 1$ alors $c(P)$ est inversible dans A et on peut supposer que $c(P) = 1$. Supposons que $P = QR$ avec Q et R dans $\mathbf{K}[X]$. En réduisant tous les coefficients de Q et de R à un même dénominateur on peut écrire $Q = \frac{\alpha}{\beta} Q'$ (α et β premiers entre eux) et $R = \frac{\gamma}{\delta} R'$ (γ et δ premiers entre eux) et de plus Q' et R' primitifs. On a donc $P = \frac{\alpha}{\beta}.\frac{\gamma}{\delta} Q'R'$ et $\beta\delta P = \alpha\gamma Q'R'$. En passant aux contenus en vertu du lemme 1 il vient $\beta\delta = \alpha\gamma$ aux inversibles près. D'où $P = Q'R'$; P étant irréductible dans $A[X]$ on en déduit que Q' ou R' sont inversibles dans $A[X]$ donc Q ou R sont inversibles dans $\mathbf{K}[X]$ et P est irréductible dans $\mathbf{K}[X]$.

Fin de la démonstration du théorème : montrons la propriété (E) dans $A[X]$. Soit $P \in A[X]$ non nul. Si $d°P = 0$ c'est clair d'après le (i) du lemme 1. Si $d°P \geq 1$, $\mathbf{K}[X]$ étant factoriel, on peut écrire $P = P_1^{\alpha_1}.P_2^{\alpha_2}...P_r^{\alpha_r}$ où les polynômes P_k sont irréductibles dans $\mathbf{K}[X]$. Comme précédemment on peut écrire $P_k = \frac{a_k}{b_k} Q_k$ avec a_k et b_k premiers entre eux dans A et Q_k dans $A[X]$ et primitifs. On obtient $\prod_{k=1}^{r} b_k^{\alpha_k} P = \prod_{k=1}^{r} a_k^{\alpha_k} Q_k^{\alpha_k}$. En passant au contenu il vient compte tenu du lemme 1 : $\prod_{k=1}^{r} b_k^{\alpha_k} = \prod_{k=1}^{r} a_k^{\alpha_k}$ à un inversible près et donc $P = u\prod_{k=1}^{r} Q_k^{\alpha_k}$ avec $u \in A^*$; de plus Q_k est primitif et irréductible dans $\mathbf{K}[X]$ donc il est irréductible dans $A[X]$ d'après le (ii) du lemme 2 ce qui prouve (E).

Pour démontrer la propriété d'unicité (U) il suffit de montrer que $A[X]$ vérifie le lemme d'Euclide d'après la proposition précédente. Soit donc $P \in A[X]$ irréductible, Q et R dans $A[X]$, tels que P divise QR. Si $P = p \in A$, p divise

$c(QR) = c(Q)c(R)$, donc p divise $c(Q)$ ou $c(R)$. Comme Q et R sont égaux à $c(Q)$ et $c(R)$ respectivement aux inversibles près on a donc p divise Q ou p divise R.

Si $d°P \geq 1$, P est irréductible dans $\mathbf{K}[X]$ d'après le (ii) du lemme 2. $\mathbf{K}[X]$ étant factoriel P divise Q ou R. Si par exemple P divise Q il existe $Q_1 \in \mathbf{K}[X]$ tel que $Q = PQ_1$. On écrit $Q_1 = (\alpha/\beta)Q_2$ avec Q_2 dans $A[X]$ primitif et α, β dans A^* premiers entre eux. Il vient $\beta Q = \alpha PQ_2$. En passant aux contenus on obtient $\beta c(Q) = \alpha$ aux inversibles près (car P et Q_2 primitifs). Enfin en écrivant $Q = c(Q)Q'$ avec Q' primitif on obtient $Q' = uPQ_2$ ($u \in A^*$) par conséquent P divise Q' donc Q dans $A[X]$ ce qui achève la démonstration.

Exemples : $\mathbb{Z}[X]$ est factoriel puisque $\mathbb{Z}$ l'est; si A est factoriel $A[X_1,..., X_n]$ aussi (par récurrence sur n) ainsi que $A[X_1,..., X_n, ...]$ (polynômes à une infinité d'indéterminées).

3.3 Anneaux principaux

Définition : Un anneau A est principal ssi :

(i) A est intègre;

(ii) tout idéal de A est principal.

La condition (ii) signifie que pour tout idéal I de A il existe $a \in A$ tel que $I = (a)$.

Remarque : dans un anneau principal qui n'est pas un corps on a, si $p \neq 0$: p est irréductible $\Leftrightarrow$ (p) est maximal parmi les idéaux propres de $A \Leftrightarrow$ (p) maximal dans l'ensemble des idéaux propres de A (puisque tout idéal est principal).

Donc, dans un anneau principal si p est non nul on a : p irréductible $\Leftrightarrow$ (p) maximal $\Leftrightarrow$ (p) premier (d'après la proposition du 3.2).

Théorème : Un anneau principal est factoriel.

Démonstration : montrons la propriété (E).

Supposons qu'il existe un élément $a_1 \in A - \{0\}$ n'admettant pas de décomposition. Alors a_1 n'est ni inversible ni irréductible. Il existe a_2 et b_2 dans A tels que $a_1 = a_2b_2$; a_1 n'ayant pas de décomposition il en est de même de a_2 ou de b_2. Supposons que ce soit a_2; on a donc $(a_1) \subset (a_2)$. Reprenant le raisonnement pour a_2 on voit qu'on peut construire par récurrence une suite $(a_1) \subset (a_2) \subset ... \subset (a_n) \subset ...$ strictement croissante d'idéaux de A. Il est clair que $I = \bigcup_{k \in N} (a_k)$ est un idéal de A. A étant principal il existe $d \in A$ tel que $I = (d)$. Comme $d \in I$, il existe $p \in \mathbb{N}$ tel que $d \in (a_p)$. On a donc $(d) \subset (a_p)$. L'inclusion inverse étant vraie on en déduit que $(d) = (a_p)$. Comme $(a_p) \subset (a_q) \subset (d)$ pour $q \geq p$ la suite (a_k) est stationnaire à partir de p ce qui n'est pas. A vérifie donc (E).

Pour montrer que A vérifie la propriété (U) il suffit de montrer que $p \in A - \{0\}$ est irréductible ssi l'idéal (p) est premier (d'après la proposition du 3.2) ce qui résulte de la remarque précédente.

La réciproque du théorème est fausse : par exemple $\mathbb{Z}[X]$ est factoriel d'après le théorème de Gauss mais pas principal (on voit facilement que l'idéal $(2, X)$ engendré par 2 et X n'est pas principal).

Proposition : Dans un anneau principal A, si a et b appartiennent à $A - \{0\}$ on a :

(i) $(a) + (b) = (\text{pgcd}(a, b))$.

(ii) a et b sont premiers entre eux ssi $(a) + (b) = A$ ssi $\exists (u, v) \in A \times A$ / $au + bv = 1$ (*Relation de Bezout*).

On retrouve par conséquent la situation de $\mathbb{Z}$.

Démonstration :

(i) démonstration analogue à celle de l'exercice 7 de « groupes »;

(ii) clair.

Remarquons que *la relation de Bezout est fausse en général* si on ne suppose pas l'anneau principal : par exemple dans $\mathbf{K}[X, Y]$ les éléments X et Y sont premiers entre eux mais $(X) + (Y) \neq \mathbf{K}[X, Y]$ (car $(X) + (Y)$ est constitué des polynômes P tels que $P(0, 0) = 0$).

Le paragraphe suivant fournit un exemple important d'anneau principal.

3.4 Anneaux euclidiens

Définition : Un anneau A est *euclidien* ssi :

(i) A est intègre;

(ii) A est muni d'une *division euclidienne*, c'est-à-dire qu'il existe une application v de $A-\{0\}$ dans $\mathbb{N}$ vérifiant :

$\forall\ a \in A, \forall\ b \in A-\{0\},\ \exists (q, r) \in A\times A$ tel que : $a = bq + r$ avec ($r = 0$ ou $v(r) < v(b)$).

L'application v s'appelle *valuation euclidienne*.

Remarque : on impose parfois à v de réaliser la condition supplémentaire : pour tous a et b de $A-\{0\}$ tels que a/b, on a $v(a) \leq v(b)$. On dit alors que v est un *stathme euclidien*.

Théorème : Tout anneau euclidien est principal.

Démonstration : c'est la même démonstration que pour montrer que les sous-groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ (« groupes » exercice 7). Soit A un anneau euclidien et I un idéal non nul de A. Soit $a \in I-\{0\}$ tel que $v(a)$ soit minimum. Soit $y \in I$. La division de y par a donne l'existence d'un couple (q, r) tel que $y = aq + r$ avec ($r = 0$ ou $v(r) < v(a)$). L'écriture $r = y - aq$ montre que r appartient à I. Par définition de a on a $r = 0$ soit $y = aq$ donc $I \subset (a)$. L'inclusion inverse étant vraie on en déduit que $I = (a)$.

Exemples : $\mathbb{Z}$ est euclidien avec $v(n) = |n|$.

Si $\mathbf{K}$ est un corps $\mathbf{K}[X]$ est euclidien : cela résulte du

lemme : Soit A un anneau et $P \in A[X]$ non nul et *de coefficient dominant inversible*; alors pour tout $F \in A[X]$ il existe $(Q, R) \in A[X]\times A[X]$ unique tel que :

$F = PQ + R$ avec $d°R < d°P$.

En particulier, si A est un corps, il existe dans $\mathbf{K}[X]$ une division euclidienne avec $v(P) = d°P$.

Démonstration du lemme : si $d°P = 0$, P est une constante inversible et le résultat est vrai (avec $R = 0$).

Raisonnons dans l'anneau quotient $A[X]/(P)$. Il s'agit de montrer la propriété :

$\forall\ F \in A[X], \exists\ R \in A[X]$ tel que ($\overline{F} = \overline{R}$ et $d°R < d°P$) (*).

Soit $P = a_nX^n + ... + a_0$ avec a_n inversible et $n \geq 1$. Il est clair qu'il suffit de montrer la propriété (*) pour $F = X^p$ ($p \in \mathbb{N}$). Vérifions-la par récurrence sur p : si $p < n$ c'est évident. Soit un entier $p \geq n$ et supposons la propriété vraie pour les entiers $< p$. Comme $\overline{X}^n = \overline{a}_n^{-1}\left(-\overline{a}_{n-1}\overline{X}^{n-1} - ... - \overline{a}_0\right)$ on a $\overline{X}^p = \overline{X}^n\overline{X}^{p-n} = \overline{a}_n^{-1}\left(-\overline{a}_{n-1}\overline{X}^{p-1} - ... - \overline{a}_0\overline{X}^{p-n}\right)$ et on conclut d'après l'hypothèse de récurrence.

Si (Q^*, R^*) est un autre couple vérifiant $F = PQ^* + R^*$ avec $d°R^* < d°P$ on a $P(Q - Q^*) = R^* - R$. Le coefficient de plus haut degré de P étant inversible on a $d°[P(Q - Q^*)] = d°P + d°(Q - Q^*) = d°(R^* - R)$. Comme $d°(R^* - R) < d°P$ on en déduit $d°(Q - Q^*) = -\infty$ soit $Q^* = Q$ puis $R = R^*$.

Remarque : on peut montrer qu'il existe des anneaux principaux non euclidiens (voir par exemple « Tauvel » p. 155).

Exercice 20

Soit K un corps et P un élément de $K[X]$ irréductible. Montrer que $L = K[X]/(P)$ est un corps. Montrer que K s'injecte dans L et que P considéré comme élément de $L[X]$ admet une racine dans L.

(on dit que L est un *corps de rupture de P dans K*).

Exemples d'anneaux euclidiens :

$\mathbb{Z}[i]$ (anneau de Gauss) (voir exercice n° IX);

$\mathbf{K}[[X]]$, anneau des séries formelles à coefficients dans $\mathbf{K}$;

Exercice 21

1°/ Montrer que $\mathbb{D} = \{A10^p / A \in \mathbb{Z}$ et $p \in \mathbb{Z}\}$, anneau des nombres décimaux est euclidien.

2°/ Plus généralement soit un anneau A commutatif intègre et S une partie de A ne contenant pas 0, contenant 1 et telle que ($x \in S$ et $y \in S \implies xy \in S$) (on dit que S est une *partie multiplicative* de A). Posons AS^{-1} la partie de $\mathbf{K} = \mathrm{Frac}(A)$ (corps des fractions de A) constitué des élément de la forme $a.s^{-1}$ où $a \in A$ et $s \in S$. Il est clair que AS^{-1} est un sous-anneau de $\mathbf{K}$ appelé *localisé de A* par rapport à S.

Montrer que si A est euclidien et muni d'un stathme euclidien il en est de même pour AS^{-1}.

Exercice 22

Montrer que $A[X]$ est principal ssi A est un corps.

(Si $a \neq 0$ considérer l'idéal I engendré par a et X).

Exercices complémentaires

I **a/** Soit A un anneau commutatif. Montrer que A admet des éléments idempotents (i.e $a^2 = a$) différents de 0 et de 1 ssi A est isomorphe à $B \times C$ où B et C sont deux anneaux non nuls (indication : si a est un tel élément alors $(1 - a)^2 = 1 - a$; considérer l'application φ de A dans $A \times (1 - a)A$ qui à u associe $(au; (1 - a)u)$ et montrer que c'est un isomorphisme d'anneaux).

b/ Soit l'anneau des fonctions continues de X dans $\mathbb{R}$. Montrer que $C(X; \mathbb{R})$ admet des nilpotents différents de O et de 1 ssi X est non connexe (indication : X non connexe ssi il existe une fonction continue non constante de X dans {0; 1}).

II Soit A un anneau factoriel tel que : $\forall (a, b) \in A \times A$, l'idéal (a, b) engendré par a et b est principal. Montrer que A est principal (indication : si I est un idéal non principal de A construire une suite strictement croissante d'idéaux principaux).

III *Anneaux noethériens*

a/ Soit A un anneau; montrer que les conditions suivantes sont équivalentes :

(i) Tout idéal de A est de type fini (i.e engendré par un nombre fini d'éléments);

(ii) Toute suite croissante d'idéaux est stationnaire;

(iii) Tout ensemble non vide d'idéaux de A possède un élément maximal pour l'inclusion.

Un anneau vérifiant l'une de ces conditions est appelé *anneau noethérien*. Par exemple tout anneau principal est noethérien.

(indication : pour (iii) $\Rightarrow$ (i), si I est un idéal de A considérer $C = \{J$ idéal de $A \ / \ J \subset I$ et J de type fini$\}$ et I_0 est un élément maximal de C, montrer que $I_0 = I$).

b/ Montrer que : A noethérien $\Rightarrow$ A/I noethérien (voir exercice 9);

Remarque : on démontre (difficile !) : A noethérien $\Rightarrow$ $A[X]$ noethérien (*théorème de transfert de Hilbert*).

c/ Montrer que si A est intègre et noethérien alors A vérifie la propriété (E) (existence de la décomposition en produit d'irréductibles) (considérer $C = \{(a) / a$ n'a pas de décomposition $\}$ et appliquer (iii)).

Application : $\mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5} \ / \ a$ et $b \in \mathbb{Z}\}$ est isomorphe à $\mathbb{Z}[X]/(X^2 + 5)$, donc vérifie (E) mais pas (U).

Plus généralement si I est un idéal premier de I et si A est noethérien alors A/I est noethérien (donc vérifie (E)).

IV Soit $A = \mathbb{C}[X, Y]/(Y - X^2)$. Montrer que A est isomorphe à $\mathbb{C}[X]$ (indication : considérer le morphisme d'anneaux φ de $\mathbb{C}[X, Y]$ dans $\mathbb{C}[X]$ qui à P associe $P(X, X^2)$ puis sa décomposition canonique).

V Montrer que $\mathbb{C}[X, Y]/(XY - 1)$ est isomorphe à l'anneau $\{ \frac{P(X)}{X^n} \ / \ n \in \mathbb{N}$ et $P \in \mathbb{C}[X]\}$ (s'inspirer de l'exercice précédent). En utilisant l 'exercice 21 montrer que cet anneau est euclidien.

VI Soit $A = \mathbb{C}[X, Y]/(Y^2 - X^3)$. Montrer que A est isomorphe à l'ensemble des polynômes de $\mathbb{C}[T]$ dont le coefficient de terme en T est nul (considérer le morphisme d'anneaux φ de $\mathbb{C}[X, Y]$ dans $\mathbb{C}[T]$ qui à P associe $P(T^2, T^3)$).

Montrer que A est intègre et noethérien et donc vérifie (E) (voir III).

Montrer que A ne vérifie pas (U) (montrer que T^6 a deux décompositions).

VII *Carrés d'un corps*

Soit F_q le corps (unique à un isomorphisme près) à $q = p^n$ éléments (voir cours) avec p premier et $n \in \mathbb{N}^*$. On pose :

$F_q^2 = \{x \in F_q \,/\, \exists\, y \in F_q$ tel que $x = y^2\}$ et $F_q^{2*} = F_q^2 - \{0\}$.

a/ Si $p = 2$ montrer que $F_q^2 = F_q$ (considérer l'homomorphisme de Fröbenius).

b/ Si $p > 2$ montrer que $|F_q^2| = \dfrac{q+1}{2}$ et $|F_q^{2*}| = \dfrac{q-1}{2}$ (considérer l'homomorphisme de groupes de F_q^2 dans F_q^2 qui à x associe x^2).

c/ En déduire que si $p > 2$ on a : $x \in F_q^{2*} \Leftrightarrow x^{\frac{q-1}{2}} = 1$, puis que :

$-1 \in F_q^{2*} \Leftrightarrow q \equiv 1\ (4)$.

d/ Montrer qu'il y-a une infinité de nombres premiers de la forme $1 + 4k$ ($k \in \mathbb{N}$).

(Raisonner par l'absurde : s'il n'en existe qu'un nombre fini soit n le plus grand d'entre eux et p un nombre premier divisant $(n!)^2 + 1$; on a $p \geq n + 1$ et dans $\mathbb{Z}/p\mathbb{Z}$: $(n!)^2 = -1$; donc -1 est un carré et donc $p \equiv 1\ (4)$).

VIII *Anneau de Gauss; somme de deux carrés*

Soit $A = \mathbb{Z}[i] = \{a + ib \,/\, a$ et $b \in \mathbb{Z}\}$.

a/ Montrer que A est un anneau commutatif, intègre, isomorphe à $\mathbb{Z}[X]/(X^2 + 1)$ (considérer le morphisme d'anneaux $P \mapsto P(i)$ de $\mathbb{Z}[X]$ dans A).

b/ Montrer que $z = a + ib \mapsto a - ib$ est un automorphisme d'anneau de A.

c/ Soit N l'application $z \mapsto z\bar{z} = a^2 + b^2$ de A dans $\mathbb{N}$. Montrer que pour tous z ei z' de A on a : $N(zz') = N(z)N(z')$ et que $N(z) = 0 \Leftrightarrow z = 0$.

d/ Précisez A^*, groupe des éléments inversibles de A.

e/ Montrer que : $\forall\, z \in A$, $\forall\, t \in A - \{0\}$, $\exists q \in A$ et $\exists\, r \in A$ tels que $z = tq + r$ et $N(r) < N(t)$.

En déduire que A est euclidien (donc principal).

On pose $\Sigma = \{n \in \mathbb{N} / \exists (a, b) \in \mathbb{N}\times\mathbb{N}$ avec $n = a^2 + b^2\}$.

f/ Montrer que si $n \equiv 3\ (4)$ alors $n \notin \Sigma$ (<u>indication</u> : un carré est congru à 0 ou 1 modulo 4).

g/ Montrer que Σ est stable par multiplication.

h/ Si p est un nombre premier, montrer que : $p \in \Sigma \Leftrightarrow p \equiv 1\ (4)$

(<u>indication</u> : montrer d'abord que : $p \in \Sigma \Leftrightarrow p$ non irréductible dans $\mathbb{Z}[i]$ puis raisonner ensuite dans $\mathbb{Z}[i]/(p)$ isomorphe à $\mathbb{Z}/p\,[X]/(X^2 + 1)$ en utilisant VIII).

i/ En déduire que si $n \in \mathbb{N} - \{0, 1\}$ et $n = \prod_{p \in P} p^{v_p(n)}$ sa décomposition en produit de facteurs premiers on a :

$n \in \Sigma \Leftrightarrow v_p(n)$ est pair pour $p \equiv 1\ (4)$.

IX *Anneau $\mathbb{Z}[\sqrt{2}]$*

On pose $\mathbb{Q}[\sqrt{2}] = \{r + r'\sqrt{2} \,/\, r$ et $r \in \mathbb{Q}\}$.

1°/ Soit N l'application de $\mathbb{Q}[\sqrt{2}]$ dans $\mathbb{R}$ qui à $z = r + r'\sqrt{2}$ (r et r' dans $\mathbb{Q}$) associe $N(z) = |r^2 - 2r'^2|$. Montrer que cette application est bien définie et que pour tous z et z' de A on a : $N(zz') = N(z)N(z')$, $N(z/z') = N(z)/N(z')$ (si $z' \neq 0$) et ($N(z) = 0 \Leftrightarrow z = 0$).

2°/ Montrer que $\mathbb{Q}[\sqrt{2}]$ est un sous-corps de $\mathbb{R}$.

On pose $A = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \,/\, a$ et $b \in \mathbb{Z}\}$.

3°/ Montrer que A est un anneau commutatif, intègre, isomorphe à $\mathbb{Z}[X]/(X^2 - 2)$ (s'inspirer du V).

4°/ Montrer que pour tout $x \in A$ et tout $y \in A - \{0\}$ il existe $(q, r) \in A\times A$ tel que :

$x = yq + r$ avec $N(r) < N(y)$.

(<u>indication</u> : déterminer $q \in A$ tel que $N\left(\frac{x}{y} - q\right) < 1$).

A est donc un anneau euclidien. Le couple (q, r)est-il unique ?

5°/ Le but de la question est de déterminer A^*, ensemble des éléments inversibles de A.

a/ Montrer que $z \in A^* \Leftrightarrow N(z) = 1$.

On pose $J = \{x \in A^* / x > 0\}$ et $K = \{x \in A^* / x > 1\}$

b/ Montrer que $K = \{a + b\sqrt{2} \in A^* / a \text{ et } b \in \mathbb{N}^*\}$. Montrer que le minimum de K est $1 + \sqrt{2}$.

c/ Montrer que $K = \{(1 + \sqrt{2})^n / n \in \mathbb{N}\}$ (<u>indication</u> : si $x \in K$ considérer l'entier naturel n tel que $(1 + \sqrt{2})^n \leq x < (1 + \sqrt{2})^{n+1}$; si l'inégalité est stricte aboutir à une contradiction en divisant par $(1 + \sqrt{2})^n$).

d/ En déduire enfin que $J = \{(1 + \sqrt{2})^n / n \in \mathbb{Z}\}$ puis que $A^* = \{\pm(1 + \sqrt{2})^n / n \in \mathbb{Z}\}$.

e/ <u>Application</u> : résoudre dans $\mathbb{Z}\times\mathbb{Z}$ les équations :

(i) $x^2 - 2y^2 = 1$;

(ii) $x^2 - 2y^2 = -1$.

X Soit A un anneau commutatif. A quelle condition nécessaire et suffisante sur A est-il vrai que pour tout entier naturel n, tout polynôme de $A[X]$ de degré n admet n racines au plus ?

(<u>Réponse</u> : A est intègre; si A n'est pas intègre et si a et b sont des diviseurs de 0, considérer le polynôme $(X - a)(X - b)$).

XI *Critère d'irréductibilité d'Eisenstein*

Soit A un anneau factoriel, K son corps des fractions et $P(X) = a_n X^n + ... + a_0 \in A[X]$. On suppose qu'il existe un élément irréductible p de A tel que :

(i) p ne divise pas a_n;

(ii) $\forall\ i \in \{0, 1, ... , n-1\}$, p divise a_i;

(iii) p^2 ne divise pas a_0.

Montrer que P est irréductible dans $K[X]$ (donc dans $A[X]$ si pgcd$(a_i) = 1$).

<u>Applications</u> :

Si p est premier, $X^{p-1} + X^{p-2} ... + X + 1$ est irréductible dans $\mathbb{Z}[X]$;

$X^4 + 1$ est irréductible dans $\mathbb{Z}[X]$ (poser $X = Y + 1$).

XII *Résultant de deux polynômes*

Soient $P = \sum_{i=0}^{p} a_i X^i$ et $Q = \sum_{j=0}^{q} b_j X^j$ deux polynômes de degrés respectifs p et $q > 0$ à coefficients dans un corps commutatif K.

1°/ Montrer que les polynômes P et Q ne sont pas premiers entre eux ssi il existe deux polynômes non nuls A et B tels que $d°A \leq q - 1$, $d°B \leq p - 1$ et $AP + BQ = 0$.

On considère l'application $\Phi_{P,Q}$ de $K_{q-1}[X] \times K_{p-1}[X]$ dans $K_{p+q-1}[X]$ définie par $\Phi_{P,Q}(U, V) = UP + VQ$. On munit d'autre part $K_{q-1}[X] \times K_{p-1}[X]$ de la base $((X^{q-1}, 0), ... , (1, 0), (0, X^{p-1}), ... , (0, 1))$ et $\boldsymbol{K}_{p+q-1}[X]$ de sa

base canonique (X^{p+q-1}, ... , 1). La matrice de $\Phi_{P,Q}$ dans ces bases est donc :

$$\begin{pmatrix} a_p & 0 & \cdots & & b_q & 0 & \cdots & 0 \\ a_{p-1} & a_p & \ddots & & b_{q-1} & b_q & & \vdots \\ \vdots & a_{p-1} & \ddots & & \vdots & b_{q-1} & \ddots & 0 \\ a_0 & \vdots & \ddots & a_p & b_0 & \vdots & \ddots & b_q \\ \vdots & a_0 & & a_{p-1} & 0 & b_0 & & b_{q-1} \\ \vdots & \vdots & & \vdots & \vdots & & & \vdots \\ \vdots & \vdots & & \vdots & \vdots & & & \\ 0 & 0 & \cdots & 0 & \cdots & \cdots & 0 & 0 \end{pmatrix}$$ (c'est une matrice carrée d'ordre (p + q)).

Le déterminant de la matrice précédente s'appelle *résultant* des polynômes P et Q. On le note res(P, Q).

2°/ Montrer que : **(i)** res(Q, P) = $(-1)^{pq}$res(P, Q); **(ii)** res(λP, μQ) = $\lambda^q \mu^p$res(P, Q) (pour λ et μ scalaires non nuls).

Montrer que les conditions suivantes sont équivalentes :

(a) P et Q sont premiers entre eux;

(b) res(P, Q) = 0.

On considère l'application Ψ_Q de l'espace vectoriel quotient E = K[X]/(P) dans lui-même et définie par $\Psi_Q(\overline{U}) = \overline{Q(X)} \times \overline{U}$. Soit la base de E : ***b*** = (1, x, ... , x^{p-1}) où x est la classe de X dans E.

3°/ a/ Déterminer la matrice de Ψ_Q dans la base **b.** En déduire que **:**

res(P, Q) = a_p^q dét(Ψ_Q) .

b/ En déduire les propriétés suivantes :

(i) si $\alpha \in K$ et $Q \in K[X]$ de degré ≥ 1 on a : res($X - \alpha$, Q) = $Q(\alpha)$;

(ii) si P, Q et $R \in K[X]$ de degré ≥ 1 on a : res(P, QR) = res(P, Q) res(P, R)

(iii) si P est scindé sur K de racines α_1, ... , α_p on a :

res(P, Q) = $a_p^q\, Q(\alpha_1) \ldots Q(\alpha_p)$.

Si de plus Q est scindé sur ***K*** de racines β_1, ... , β_q on a :

$$\text{res}(P, Q) = a_p^q b_q^p \prod_{i=1}^{p} \prod_{j=1}^{q} (\alpha_i - \beta_j)$$

4°/ <u>Exemple d'application</u> : Soient deux polynômes P et Q premiers entre eux. Alors il existe un voisinage V_P de P et V_Q de Q tel que tout polynôme de V_P est premier avec tout polynôme de V_Q. (Autrement dit en "bougeant un peu les coefficients de deux polynômes premiers entre eux, ils restent premiers entre eux).

XIII *Groupe multiplicatif d'un corps*

Soit K un corps commutatif et G un sous-groupe fini du groupe multiplicatif (K^*, ×). On pose n = |G|, E_d = { $x \in G$ / x^d = 1} et Γ_d = { $x \in G$ / x est d'ordre d dans G}.

1°/ Montrer que : $\Gamma_d \neq \varnothing \Leftrightarrow |\Gamma_d| = \varphi(d)$ où φ est la fonction indicatrice d'Euler (voir exposé « groupes »).

(Montrer que si $\Gamma_d \neq \varnothing$ et $x \in \Gamma_d$ on a : <x> = E_d).

2°/ Montrer que $n = \sum_{d/n} |\Gamma_d|$

3°/ En déduire que pour tout diviseur d de n on a : $|\Gamma_d| = \varphi(d)$ (utiliser que $n = \sum_{d/n} \varphi(d)$: voir exposé « groupes »).

Conclure que <u>*tous sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique*</u>.

<u>Application</u> : si p est un nombre premier : $(\mathbb{Z}/p\mathbb{Z})^*$ est isomorphe à $\mathbb{Z}/(p-1)\ \mathbb{Z}$.

4°/ Démontrer le résultat précédent en utilisant que dans un groupe fini commutatif il existe un élément ayant pour ordre le ppmc des ordres des éléments de ce groupe (voir exercice 11 du chapitre "Groupes").

XIV Si K et L sont des corps tels que $K \subset L$ on dit que L est une *extension de K.* Un élément a de L est *algébrique sur K* s'il existe un polynôme P non nul à coefficients dans K tel que $P(a) = 0$; si a n'est pas algébrique on dit qu'il est *transcendant sur K*.

D'autre part Si $a \in L$ on note $K(a)$ le plus petit sous-corps contenant K et a.

1°/ Soit a un élément de L algébrique sur K. Montrer qu'il existe un unique polynôme P_0 de $K[X]$ caractérisé par : pour tout polynôme P de $K[X]$ on a : $P(a) = 0 \Leftrightarrow P$ multiple de P_0.

P_0 est appelé *polynôme minimal de a sur K*.

2°/ Montrer que les conditions suivantes sont équivalentes :

(i) a est algébrique sur K de polynôme minimal P_0;

(ii) $K(a) = K[a]$ $(= \{P(a) / P \in K[X]\}$;

(iii) $K[a]$ est un espace vectoriel de dimension finie sur K (plus précisément $\dim_K K[a] = d°P_0$).

(considérer le morphisme d'anneaux φ de $K[X]$ dans $K[a]$ qui à P associe $P(a)$ pour (i) $\Rightarrow$ (ii)).

Chap. 2 Anneaux et corps

Exercice 1

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont intègres. $\mathbb{Z}/4\mathbb{Z}$ par exemple n'est pas intègre puisque $\overline{2}.\overline{2} = \overline{0}$ et $\overline{2} \neq \overline{0}$.

Plus généralement montrons que $\mathbb{Z}/n\mathbb{Z}$ est intègre ssi $n = 0$ ou n est premier.

Si $n = 0$ alors $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}$ qui est intègre. Si $n = 1$ $\mathbb{Z}/n\mathbb{Z} = \{0\}$ qui par définition n'est pas intègre.

Si $n > 1$ n'est pas premier il existe deux entiers a et b différents de 1 tels que $a.b = n$. Donc $\overline{a}.\overline{b} = \overline{0}$ et $\overline{a}$ et $\overline{b}$ sont distincts de $\overline{0}$ donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.

Inversement si n est premier $(\mathbb{Z}/n\mathbb{Z} - \{\overline{0}\}, \overline{\times})$ est un groupe (« groupes, exercice 1) et donc $\mathbb{Z}/n\mathbb{Z}$ n'a pas de diviseurs de 0.

$F(E, A)$ n'est pas intègre en général : par exemple si $E = A = \mathbb{R}$, soit $f \in F(\mathbb{R}, \mathbb{R})$ qui vaut 1 sur $\mathbb{R}_+$ et 0 ailleurs et $g = 1 - f$. Alors les applications f et g sont non nulles et $f \times g = \mathbf{O}$, application nulle de $\mathbb{R}$ dans $\mathbb{R}$.

Montrons que $A[X]$ est intègre ssi A est intègre.

Supposons A intègre. La fonction degré vérifie alors pour tous polynômes P et Q : $d°(PQ) = d°P + d°Q$ (on convient que le degré du polynôme nul est $-\infty$). Si $PQ = 0$, en prenant le degré il vient $d°P + d°Q = -\infty$ donc $d°P$ ou $d°Q = -\infty$ i.e $P = 0$ ou $Q = 0$ et $A[X]$ est intègre.

Si $A[X]$ est intègre il est clair que A aussi.

$L(E)$ et $M_n(A)$ ne sont pas intègres en général : par exemple $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Si Card $E \geq 2$, $(P(E), \Delta, \cap)$ n'est pas intègre : on peut avoir $A \cap B = \varnothing$ et A et B non vide.

Exercice 2

Soit A un anneau fini intègre et $a \in A - \{0\}$. Considérons l'application f de A dans A qui à x associe $a.x$. Cette application est injective car pour tout x et x' de A : $f(x) = f(x')$ ssi $a.x = a.x'$ ssi $a.(x - x') = 0$, soit $x - x' = 0$ puisque A est intègre et $a \neq 0$. A étant un ensemble fini f est donc une bijection de A dans A : il existe $a' \in A$ tel que $f(a') = 1$, soit $a.a' = 1$. De même en considérant l'application qui à x associe $x.a$ on montre qu'il existe $a'' \in A$ tel que $a''.a = 1$.

Mais $(a'a)a'' = 1a'' = a''$ d'une part et $a'(aa'') = a'1 = a'$ d'autre part, donc $a'' = a'$ qui est l'inverse de a. Tout élément non nul de A ayant un inverse, A est un corps.

Exercice 3

D'après l'exercice 2 un anneau fini A est un corps ssi il est intègre. Si n est un entier naturel non nul on a donc $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi $\mathbb{Z}/n\mathbb{Z}$ est intègre ce qui équivaut à n premier d'après l'exercice 1.

Exercice 4

On montre facilement que $K = \{a + b\sqrt{2} \ / \ a \text{ et } b \in \mathbb{Q}\}$ est un sous-corps de $\mathbb{R}$.

Exercice 5

En effet si I est un idéal de $\mathbb{Z}$ c'est un sous-groupe de $\mathbb{Z}$ donc il existe $n \in \mathbb{Z}$ tel que $I = n\mathbb{Z}$ (voir « groupes » exercice 7); réciproquement on vérifie immédiatement que $n\mathbb{Z}$ est bien un idéal de $\mathbb{Z}$.

Exercice 6

Soit A est un corps et I est un idéal à gauche de A non nul. Soit $a \in I - \{0\}$. Alors $a^{-1}a \in I$ donc $1 \in I$ soit $I = A$. De même si I est un idéal à droite. D'où la condition nécessaire.

Réciproquement soit A un anneau où tout idéal à gauche est trivial. Soit $a \in A - \{0\}$. L'ensemble $I_a = \{xa / x \in A\}$ est un idéal à gauche de A. Comme $(a) \neq (0)$ on a $(a) = A$ d'après l'hypothèse. Il existe donc $x \in A$ tel que $xa = 1$. x est

donc non nul et le même raisonnement montre qu'il existe $y \in A$ tel que $yx = 1$. On a $y = yxa =$ a donc $xa = xa = 1$ et a est donc inversible. Tout élément non nul de A a donc un inverse et A est un corps.

Démonstration analogue si les idéaux à droite sont triviaux.

Exercice 7

Notons d'abord que dans un anneau quotient A/I on a une loi externe définie pour tout a et x de A par $a\overline{x} = \overline{ax}$ (cette définition est légitime car $x - x' \in I \Rightarrow ax - ax' \in I$). Dans l'anneau $B = \mathbf{K}[X]/(P(X) - X)$ on a alors pour tout polynôme Q : $Q\left(\overline{X}\right) = \overline{Q(X)}$ puis : $\overline{P(P(X)) - X} = \overline{P(P(X))} - \overline{X} = P\left(\overline{P(X)}\right) - \overline{X} = P\left(\overline{X}\right) - \overline{X} = \overline{P(X)} - \overline{X} = \overline{0}$ (où on a utilisé que $\overline{P(X)} = \overline{X}$) d'où le résultat.

Exercice 8

Si f est un morphisme d'anneaux de A dans B on a pour tout a de A et tout x de Ker f : $f(a.x) = f(a).f(x) = 0_B$ (car $f(x) = 0_B$) donc $a.x \in$ Ker f. Comme de plus Ker f est un sous-groupe de A c'est donc un idéal de A.

Si J est un idéal de B, $f^{-1}(J)$ est un sous-groupe de A et pour tout a de A et tout x de $f^{-1}(J)$ on a : $f(a.x) = f(a).f(x) \in J$ (car J est un idéal de B). Donc $f^{-1}(J)$ est un idéal de A.

Remarque : soit f de $\mathbb{Z}[X]$ dans lui-même qui à P associe $P(2X)$: c'est un morphisme d'anneaux. L'image de l'idéal $\mathbb{Z}[X]$ n'est pas un idéal de $\mathbb{Z}[X]$ car $1 \in f(\mathbb{Z}[X])$ mais $1.X \notin f(\mathbb{Z}[X])$. L'image directe d'un idéal par un morphisme d'anneaux n'est donc pas toujours un idéal.

Exercice 9

Soit S l'application qui à un idéal J de A contenant I associe $\overline{J} = \{\overline{x} / x \in J\}$ (où $\overline{x}$ est la classe de x dans A/I). Il est clair que $\overline{J}$ est un idéal de A/I. D'autre part si $\mathcal{J}$ est un idéal de A/I, $S^{-1}(\mathcal{J})$ est un idéal de A (exercice 8) contenant I donc S est une surjection de l'ensemble des idéaux de A contenant I dans l'ensemble des idéaux de A/I.

Soient J et J' sont deux idéaux de A contenant I tels que $S(J) = S(J')$. Si $y \in J$ on a $\overline{y} \in \overline{J}$ donc $\overline{y'} \in \overline{J'}$ c'est-à-dire qu'il existe $y' \in J'$ et $z \in I$ tels que $y = y' + z$. Comme $z \in I \subset J'$ on a $y \in J'$ soit $J \subset J'$. De même $J' \subset J$ donc S est injective. C'est donc une bijection de l'ensemble des idéaux de A contenant I dans l'ensemble des idéaux de A/I.

Exercice 10

f étant considérée comme un morphisme de groupes on a la décomposition $f = i \circ \overline{f} \circ s$ où $\overline{f}$ est un isomorphisme de groupes. D'autre part pour tous x et y de A/Ker f on a $\overline{f}(\overline{x}.\overline{y}) = \overline{f}\left(\overline{xy}\right) = f(x.y)$ (par définition de $\overline{f}$) et $f(x.y) = f(x).f(y) = \overline{f}(\overline{x})\overline{f}(\overline{y})$ donc $\overline{f}$ est un isomorphisme d'anneaux.

Exercice 11

Soit $A = \{a + b\sqrt{2} / a \text{ et } b \in \mathbb{Q}\}$ et considérons l'application φ de $\mathbb{Q}[X]$ dans A qui à P associe $P(\sqrt{2})$. Il est clair que φ est un morphisme d'anneaux surjectif. Soit P appartenant au noyau de φ. La division euclidienne de P par $X^2 - 2$ donne $P = (X^2 - 2)\,Q + R$ où $(Q, R) \in \mathbb{Q}[X]^2$ et $d°R < 2$. Il existe donc a et b dans $\mathbb{Q}$ tels que $R = aX + b$, soit $P(\sqrt{2}) = a\sqrt{2} + b = 0$ d'où $a = b = 0$. Donc Ker $\varphi = (X^2 - 2)$ et $\overline{\varphi}$ est un isomorphisme de $\mathbb{Q}[X]/(X^2 - 2)$ dans A.

De même on démontre que $\mathbb{C}$ est isomorphe à $\mathbb{R}[X]/(X^2 + 1)$ en considérant l'application de $\mathbb{C}$ dans $\mathbb{R}[X]$ qui à P associe $P(i)$.

Exercice 12

K' contient 1 donc il contient $n.1$ pour tout n de $\mathbb{Z}$ i.e il contient $\varphi(\mathbb{Z})$. Si car(K) = 0, $\varphi(\mathbb{Z})$ est isomorphe à $\mathbb{Z}$ et K' est l'ensemble des $\varphi(m)/\varphi(q)$ où $(m, q) \in \mathbb{Z}\times\mathbb{Z}^*$ donc l'application de $\mathbb{Q}$ dans K' qui à m/q associe $\varphi(m)/\varphi(q)$ est un isomorphisme de $\mathbb{Q}$ dans K'.

Si car(K) = $p \neq 0$, $\varphi(\mathbb{Z})$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ qui est un corps car p est premier; ainsi $\varphi(\mathbb{Z})$ est un corps inclus dans K' donc $\varphi(\mathbb{Z}) = K'$.

Exercice 13

Soit K un corps fini de caractéristique p. K peut être considéré comme un espace vectoriel sur son corps premier K' (exercice 12). K étant fini sa dimension n aussi et donc K est isomorphe à l'espace vectoriel K'^n d'où Card $K = p^n$.

Exercice 14

Soit F l'application de K dans K qui à x associe x^p. Pour tous x et y de K on a $(x.y)^p = x^p.y^p$ car K est commutatif et d'après la formule du Binôme de Newton on a $(x + y)^p = \sum_{k=0}^{p} C_p^k x^k y^{p-k}$. Soit $0 < k < p$ posons $C_p^k = b$ donc

$p.(p-1)...(p-k+1) = b.k!$. p divise le premier membre donc il divise $b.k!$; p étant premier il est premier avec 2, 3, ... , k donc avec le produit $k!$ (« Groupes », exercice 7) donc p divise b d'après le théorème de Gauss. Par suite $C_p^k x^k y^{p-k} = 0$ pour $0 < k < p$ (le corps K étant de caractéristique p) soit $(x + y)^p = x^p + y^p$. F est donc un homomorphisme de corps.

Comme F est injective F est bijective si K est fini et c'est donc un isomorphisme dans ce cas.

Si $K = \mathbb{Z}/p\mathbb{Z}$ pour tout x de $\{0, 1, ... , p-1\}$: $x^{p-1} \equiv 1\ (p)$ (théorème de Fermat) donc $\overline{x}^p = \overline{x}$ et F est l'identité dans ce cas.

Exercice 15

On sait que si J est un idéal de B alors $f^{-1}(J)$ est un idéal de A (exercice 8). On a $x.y \in f^{-1}(J)$
$\Leftrightarrow f(x.y) \in J \Leftrightarrow f(x).f(y) \in J \Leftrightarrow f(x) \in J$ ou $f(y) \in J$ car J est premier, soit : $x \in f^{-1}(J)$ ou $y \in f^{-1}(J)$ et donc $f^{-1}(J)$ est premier d'après la caractérisation de la proposition précédente.

Autre façon : l'application F de A dans B/J qui à x associe $\overline{f(x)}$ est un homomorphisme d'anneaux dont le noyau est $f^{-1}(J)$. En considérant sa décomposition canonique $\overline{F}$ est un morphisme d'anneaux injectif de $A/f^{-1}(J)$ dans B/J. B/J étant intègre $A/f^{-1}(J)$ aussi donc $f^{-1}(J)$ est premier dans A s'il est différent de A.

Exercice 16

Si J est un idéal maximal de B c'est un idéal premier de B est donc si $f^{-1}(J)$ est différent de A c'est un idéal premier de A d'après l'exercice 15. Ce n'est pas un idéal maximal de A en général comme le montre l'exemple de l'injection de $\mathbb{Z}[X]$ dans $\mathbb{R}[X]$ et $J = (X)$: J est maximal car $\mathbb{R}[X]/(X)$ est isomorphe à $\mathbb{R}$ qui est un corps et (X) n'est pas maximal dans $\mathbb{Z}$ car $\mathbb{Z}[X]/(X)$ est isomorphe à $\mathbb{Z}$ qui est intègre sans être un corps.

Si f est surjective l'application $\overline{F}$ de $A/f^{-1}(J)$ dans B/J considérée dans l'exercice 15 est un isomorphisme d'anneaux. B/J étant un corps $A/f^{-1}(J)$ aussi et par suite $f^{-1}(J)$ est un idéal maximal de A (si $f^{-1}(J)$ est différent de A).

Exercice 17

1°/ Si x et y appartiennent à I et J respectivement le produit $x.y$ appartient à $I \cap J$ donc $IJ \subset I \cap J$ par définition de IJ.

2°/ Si I et J sont étrangers il existe $a \in I$ et $b \in J$ tels que $a + b = 1$. Soit z appartenant à $I \cap J$. On a $z = za + zb$; za et zb appartiennent à IJ donc z aussi et par suite $IJ = I \cap J$.

Si I et J sont deux idéaux distincts et si I est maximal $I + J$ est un idéal de A qui contient strictement I donc $I + J = A$ car I est maximal et I et J sont étrangers.

3°/ Considérons le cas $n = 2$. D'après la question précédente $I_1.I_2 = I_1 \cap I_2$. Soit f l'application de A danst $A/I_1 \times A/I_2$ qui à x associe $\left(\overline{x}^{I_1}, \overline{x}^{I_2}\right)$. C'est un morphisme d'anneaux et de A-modules dont le noyau est $I_1 \cap I_2$ donc l'application quotient $\overline{f}$ de $A/I_1 \cap I_2$ dans $A/I_1 \times A/I_2$ est injective.

Montrons que $\overline{f}$ est surjective. Tout élément $\left(\overline{x}^{I_1}, \overline{x}^{I_2}\right)$ de $A/I_1 \times A/I_2$ s'écrivant $x\left(\overline{1}^{I}, \overline{0}^{J}\right) + y\left(\overline{0}^{I}, \overline{1}^{J}\right)$ il suffit de montrer que $\left(\overline{1}^{I_1}, \overline{0}^{I_2}\right)$ et $\left(\overline{0}^{I_1}, \overline{1}^{I_2}\right)$ ont un antécédent. Les idéaux I_1 et I_2 étant étrangers il existe a et b dans I_1 et I_2 respectivement tels que $a + b = 1$; l'élément $z = b = 1 - a$ vérifie alors $\overline{z}^{I_1} = \overline{1}^{I_1}$ et $\overline{z}^{I_2} = \overline{0}^{I_2}$. De même $w = a = 1 - b$ vérifie $\overline{w}^{I_1} = \overline{0}^{I_1}$ et $\overline{w}^{I_2} = \overline{1}^{I_2}$ d'où la surjectivité de $\overline{f}$.

On déduit le cas général du

Lemme : si un idéal I est étranger avec les idéaux $I_1, I_2, \dots, I_n$ il est étranger avec leur produit $I_1.I_2 \dots I_n$.

En effet on dispose de n relations $u_k + v_k = 1$ avec $u_k \in I$ et $v_k \in I_k$. En les multipliant membres à membres il vient une relation du type $u + v_1v_2 \dots v_n = 1$ où $u \in I$ et $v_1v_2 \dots v_n \in I_1.I_2 \dots I_n$ d'où le lemme ce qui achève la démonstration.

Exercice 18

Condition nécessaire : soit A un anneau local, I son idéal maximal et N d'ensemble de ses éléments non inversible. Soit x un élément de N. L'idéal (x) engendré par x est un idéal propre de A donc il est contenu dans un idéal maximal J d'après le théorème de Krull. A étant local on a $J = I$ donc $x \in I$. Donc $N \subset I$; I étant un idéal distinct de A on a aussi l'inclusion inverse. $N = I$ est ainsi un idéal de A.

Condition suffisante : si l'ensemble des éléments non inversible N de A est un idéal et si J est un idéal contenant N et distinct de N, alors J contient des éléments inversibles donc $J = A$ et N est maximal. Si K est un autre idéal maximal on a $K \neq A$ et de même $K \subset N$ donc $K = N$.

Exercice 19

L'unicité de la décomposition montre que pour tout p irréductible dans A et tous a et b de $A - \{0\}$ on a $v_p(ab) = v_p(a) + v_p(b)$.

Si a/b il existe $c \in A$ tel que $b = ac$ donc pour tout p irréductible $v_p(b) = v_p(ac) = v_p(a) + v_p(c)$ donc $v_p(a) \leq v_p(b)$.

Réciproquement si pour tout $p \in P$: $v_p(a) \leq v_p(b)$ alors $b = u \prod_{p\in P} p^{v_p(b)} = u \prod_{p\in P} p^{v_p(a)}.\prod_{p\in P} p^{v_p(b)-v_p(a)}$ donc a divise b.

On a pour tous a et b non nuls de A : $(a) = (b) \Leftrightarrow a/b$ et $b/a \Leftrightarrow \forall\ p \in P : v_p(a) = v_p(b)$ d'après la question précédente.

Exercice 20

$\mathbf{K}[X]$ étant principal on a P irréductible $\Rightarrow (P)$ maximal donc $L = \mathbf{K}[X]/(P)$ est un corps. Il est clair que l'application de $\mathbf{K}$ dans L qui à x associe $\overline{x}$ est un morphisme injectif d'anneaux.

D'autre part on a $P\left(\overline{X}\right) = \overline{0}$ donc $\overline{0}$ est racine de P dans L.

Exercice 21

1°/ Soit $S = \{2^p5^q / p \text{ et } q \in \mathbb{Z}\}$. Tout élément de $\mathbb{D}$ s'écrit de façon unique $A.s$ où $A \in \mathbb{Z}$ premier avec 2 et 5, $s \in S$. Soit alors w l'application de $\mathbb{D}^*$ dans $\mathbb{N}$ qui à $x = A.s$ associe $|A|$. Notons que si x s'écrit $B.t$ avec $B \in \mathbb{Z}$ et $t \in S$ alors $w(x) \leq |B|$ (en effet B s'écrit $2^p.5^q.C$ avec p et q entiers naturels, $C \in \mathbb{Z}$ et C premier avec 2et 5; alors $w(x) = w(2^p.5^q.C.t) = |2^p.5^q.C| \leq B$). Soient $(a, b) \in \mathbb{D}\times\mathbb{D}$, b non nul et posons $a = A.s$ et $b = B.t$ avec A et B entiers relatifs premiers avec 2 et 5 et $(s, t) \in S \times S$. Il existe $(Q, R) \in \mathbb{Z}\times\mathbb{Z}$ tel que $A = BQ + R$ et $R = 0$ ou $|R| < |B|$. On en déduit $A.s = (B.t)(Q.st^{-1}) + R.s$ soit $a = b(Q.st^{-1}) + R.s$ avec $R.s = 0$ ou $w(R.s) \leq |R| < |B| = w(b)$ et donc $\mathbb{D}$ est euclidien.

2°/ Posons $B = AS^{-1}$. Si B est un corps le résultat est vrai.

Sinon soit P un système de représentants des éléments irréductibles de A. Soit P' le sous-ensemble de P constitué des éléments de P qui n'interviennent pas dans la décomposition en produit de facteurs irréductible d'un élément de S. B n'étant pas un corps on a $P' \neq \varnothing$ (sinon pour tout p irréductible de A il existe $s \in S$ tel que $s = pq$ donc $1 = pqs^{-1}$ d'où p est inversible dans B; par suite tout élément non nul de B serait inversible dans B). Tout élément de B s'écrit alors comme produit d'éléments de P' et d'éléments inversibles de B (puisque tout élément de S est inversible ainsi que tout élément de $P - P'$).

Supposons que $x \in B$ s'écrive $x = a.s = b.t$ avec a et b produit d'éléments de P', s et t inversibles dans B. On écrit $a = bts^{-1}$. Posons $ts^{-1} = c/u$ avec $c \in A$ et $u \in S$. On a : $bc = ua$, donc u divise bc et comme u est premier avec b il divise c donc $ts^{-1} \in A$ et par suite b divise a. En écrivant $b = ast^{-1}$ on montre de même que a divise b. v étant un stathme on a $v(a) = v(b)$. On peut ainsi définir une application w de B^* dans $\mathbb{N}$ qui à $x = a.s$ associe $v(a)$. On vérifie facilement que si x/y alors $w(x) \leq w(y)$.

Soit maintenant $y = b.t$ non nul avec les même notations que précédemment. Il existe $(q, r) \in A\times A$ tel que $a = bq + r$ avec $r = 0$ ou $v(r) \leq v(b)$. D'où $a.s = b.t(qt^{-1}s) + r.s$ soit $x = y(qt^{-1}s) + r.s$ et $r.s = 0$ ou $w(r.s) \leq v(r) < v(b) = w(y)$.

Exercice 22

D'après le cours il suffit de montre la condition nécessaire. Supposons donc que $A[X]$ soit principal. Comme $A[X]$ est intègre, A aussi. Par des considérations de degré on voit facilement que X est irréductible donc l'idéal (X) est maximal et $A[X]/(X)$ est un corps. Or, comme dans l'exercice 11, on montre que $A[X]/(X)$ est isomorphe à A (passer au quotient l'injection canonique de A dans $A[X]$) donc A est un corps.

Autre démonstration : soit $a \in A - \{0\}$. L'idéal $I = (X, a)$ engendré par X et a est principal et engendré par $P \in A[X]$. Comme $a \in I$ il existe $Q \in A[X]$ tel que $a = PQ$. En considérant le degré des deux membres on en déduit que $P = b$ = constante non nulle. De même $X \in I$ donc il existe $b' \in A$ tel que $X = b(b'X)$ soit $bb' = 1$ et b est inversible d'où $I = A$. Par conséquent $1 \in (X, a)$ et il existe Q et Q' dans $A[X]$ tels que $1 = XQ + aQ'$; si a' est le terme de plus bas degré de Q' on en déduit que $1 = aa'$ et donc a est inversible. A est donc un corps.

Correction des exercices complémentaires

I **a/** Soit A un anneau commutatif. Montrer que A admet des éléments idempotents (i.e $a^2 = a$) différents de 0 et de 1 ssi A est isomorphe à $B \times C$ où B et C sont deux anneaux non nuls (indication : si a est un tel élément alors $(1 - a)^2 = 1 - a$; considérer l'application φ de A dans $A \times (1 - a)A$ qui à u associe $(au; (1 - a)u)$ et montrer que c'est un isomorphisme d'anneaux).

b/ Soit l'anneau des fonctions continues de X dans $\mathbb{R}$. Montrer que $C(X; \mathbb{R})$ admet des nilpotents différents de O et de 1 ssi X est non connexe (indication : X non connexe ssi il existe une fonction continue non constante de X dans {0; 1}).

a/ Condition nécessaire : claire car si A est de la forme $B \times C$ on a $(1, 0)^2 = (1, 0)$.

Condition suffisante : soit a un élément idempotent et considérons l'application φ de A dans $aA \times (1 - a)A$ qui à x associe $(ax, (1 - a)x)$. On a, pour tous éléments x et y de A, $\varphi(x + y) = \varphi(x) + \varphi(y)$ et $\varphi(x.y) = (a^2xy, (1 - a)^2xy) = (axy, (1 - a)xy)$, car $a^2 = a$ et $(1 - a)^2 = 1 + a^2 - 2a = 1 + a - 2a = 1 - a$. De plus $\varphi(1) = (a, 1 - a)$ pour tout élément $(ax, (1 - a)x)$ de $aA \times (1 - a)A$: $(a, 1 - a)$. $(ax, (1 - a)x) = (a^2x, (1 - a)^2x) = (ax, (1 - a)x) = (ax, (1 - a)x).(a, 1 - a)$, donc $(a, 1 - a)$ est l'élément neutre pour la multiplication. Ainsi φ est un endomorphisme d'anneaux de A dans $aA \times (1 - a)A$.

D'autre part, pour $x \in A$: $\varphi(x) = (0, 0)$ ssi $ax = (1 - a)x = 0$, d'où $x = 0$ donc φ est injective. Enfin si $(ax, (1 - a)y) \in aA \times (1 - a)A$ on a $\varphi(ax + (1 - a)y) = (a^2x + a(1 - a)y, (1 - a)ax + (1 - a)^2y) = (ax, (1 - a)y)$ donc φ est surjective.

b/ Soit f une fonction de $C(X; \mathbb{R})$ idempotente et différente de 0 et de 1. Cela équivaut à $f.(1 - f) = 0$, i.e. f est une fonction continue à valeurs dans {0, 1} non constante ce qui équivaut à X non connexe.

II Soit A un anneau factoriel tel que : $\forall (a, b) \in A \times A$, l'idéal (a, b) engendré par a et b est principal. Montrer que A est principal (indication : si I est un idéal non principal de A construire une suite strictement croissante d'idéaux principaux).

Soit I un idéal de A non principal et $a_1 \in I$. On a $(a_1) \neq I$ donc il existe $b_1 \in I$ tel que $b_1 \in I - (a_1)$. Par hypothèse l'idéal (a_1, b_1) est principal donc il existe $a_2 \in I$ tel que $(a_1, b_1) = (a_2)$. On a donc $(a_1) \subset (a_2)$ l'inclusion étant stricte. En itérant le procédé on construit une suite strictement croissante d'idéaux (a_k) $(k \geq 1)$ de A. Soit $a_1 = u \prod_p p^{v_p(a_1)}$ la décomposition de (a_1) en produit d'éléments irréductibles de A (où P est un système de représentants des éléments irréductibles de A : voir remarque du 3.2). Pour tout entier $k \geq 1$ on a $(a_1) \subset (a_k)$ donc a_k divise a_1. Il en résulte que pour tout $p \in P$ on a $v_p(a_k) \leq v_p(a_1)$ et donc, à des inversible près, il n'y a qu'un nombre fini d'éléments a_k donc un nombre fini d'idéaux (a_k) ce qui contredit que la suite (a_k) est strictement croissante.

III *Anneaux noethériens*

a/ Soit A un anneau; montrer que les conditions suivantes sont équivalentes :

(i) Tout idéal de A est de type fini (i.e engendré par un nombre fini d'éléments);

(ii) Toute suite croissante d'idéaux est stationnaire;

(iii) Tout ensemble non vide d'idéaux de A possède un élément maximal pour l'inclusion.

Un anneau vérifiant l'une de ces conditions est appelé *anneau noethérien*. Par exemple tout anneau principal est noethérien.

(indication : pour (iii) $\Rightarrow$ (i), si I est un idéal de A considérer $C = \{J$ idéal de A / $J \subset I$ et J de type fini$\}$ et I_0 est un élément maximal de C, montrer que $I_0 = I$).

b/ Montrer que : A noethérien $\Rightarrow$ A/I noethérien (voir exercice 9);

Remarque : on démontre (difficile !) : A noethérien $\Rightarrow$ $A[X]$ noethérien (*théorème de transfert de Hilbert*).

c/ Montrer que si A est commutatif intègre et noethérien alors A vérifie la propriété (E) (existence de la décomposition en produit d'irréductibles) (considérer $C = \{(a)$ / a n'a pas de décomposition $\}$ et appliquer (iii)).

Application : $\mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5} \ / \ a \text{ et } b \in \mathbb{Z}\}$ est isomorphe à $\mathbb{Z}[X]/(X^2 + 5)$, donc vérifie (*E*) mais pas (*U*).

Plus généralement si *I* est un idéal premier de *I* et si *A* est noethérien alors *A*/*I* est noethérien (donc vérifie (*E*)).

a/ (i) $\Rightarrow$ **(ii) :** supposons que tout idéal de *A* soit de type finit soit (I_k) $(k \geq 0)$ une suite croissante d'idéaux. Il est clair que $J = \bigcup_{k\geq 0} I_k$ est un idéal de *A*. Par hypothèse il existe des éléments $x_1, \ldots, x_n$ de *A* tel que $J = (x_1, \ldots, x_n)$ (idéal engendré par $x_1, \ldots, x_n$). Soit $m = \text{Max}\{k \in \mathbb{N} \ / \ x_1, \ldots, x_n \in I_k\}$. On a $J \subset I_m$ et si $k \geq m$, $J \subset I_m \subset I_k$ car la suite (I_k) est croissante. Comme $I_k \subset J$ il en résulte que $I_k = J$ pour $k \geq m$, i.e. est stationnaire.

(ii) $\Rightarrow$ **(iii) :** supposons que toute suite croissante d'idéaux de *A* soit stationnaire et soit Γ un ensemble non vide d'idéaux de *A* n'ayant pas d'éléments maximal pour l'inclusion. Soit $I_1 \in \Gamma$. Il existe I_2 dans Γ tel que $I_1 \subset I_2$ et $I_1 \neq I_2$ (sinon I_1 serait maximal). En itérant on construit une suite d'éléments de Γ strictement croissante d'idéaux de *A* ce qui contredit l'hypothèse.

(iii) $\Rightarrow$ **(i) :** supposons que tout ensemble non vide d'idéaux de *A* possède un élément maximal pour l'inclusion et soit *I* un idéal de *A*. Considérons l'ensemble ϑ des idéaux de *A* de type fini et contenus dans *I*. ϑ est non vide car il contient $\{0\}$ donc il admet un élément maximal I_0. I_0 est donc de type fini et $I_0 \subset I$. Si *I* n'était pas inclus dans I_0 il existerait $x \in I - I_0$. Alors l'idéal $I_0 + (x)$ engendré par *I* et *x* est de type fini, est contenu dans *I* donc il appartient à ϑ et il contient strictement I_0 ce qui contredit que I_0 est maximal. On a donc $I_0 = I$ et *I* est de type fini.

b/ Soit $\left(\overline{I_k}\right)$ une suite croissante d'idéaux de *A*/*I* où I_k désigne une suite d'idéaux de *A* telle que $I \subset I_k$ et $\overline{I_k}$ l'image de I_k par la surjection canonique *s* de *A* dans *A*/*I* (voir exercice 9). La suite $s^{-1}(\overline{I_k})$ est alors une suite croissante d'idéaux de *A*, elle est donc stationnaire (a/ (ii)) : $\exists N \in \mathbb{N} \ / \ s^{-1}(\overline{I_k}) = s^{-1}(\overline{I_N})$ pour $k \geq N$. On alors, pour $k \geq N$, $s \circ s^{-1}(\overline{I_k}) = s \circ s^{-1}(\overline{I_N})$ soit $\overline{I_k} = \overline{I_N}$ (*s* étant surjective on a $s \circ s^{-1}(\overline{I_k}) = \overline{I_k}$ pour tout *k*) et donc *A* est noethérien.

c/ Soit $\vartheta = \{(a) / \ a \in A, a \neq 0$ et *a* ne vérifie pas la propriété **(E)**$\}$ (voir 3.2). Supposons ϑ non vide. L'anneau *A* étant supposé noethérien il admet un élément maximal (*c*) d'après a/ (iii).

c ne vérifie pas la propriété **(E)** donc en particulier il est non inversible et non irréductible et il existe deux éléments c_1 et c_2 de *A* non inversibles tels que $c = c_1 c_2$. On en déduit que $(c) \subset (c_1)$ et $(c) \subset (c_1)$ les inclusions étant strictes. Mais c_1 ou c_1 ne vérifie pas la propriété **(E)** (sinon *c* vérifierait cette propriété) : cela contredit que (*c*) est un élément maximal de ϑ. En conclusion ϑ est vide et *A* vérifie la propriété **(E)**.

Application : $\mathbb{Z}$ est principal donc noethérien (tout idéal est de type fini) donc $\mathbb{Z}[X]$ est noethérien (d'après b/) donc $\mathbb{Z}[X]/(X^2 + 5)$ aussi. Or les anneaux $\mathbb{Z}[X]/(X^2 + 5)$ et $\mathbb{Z}[i\sqrt{5}]$ sont isomorphes (même démonstration que dans l'exercice 11 du cours) donc $\mathbb{Z}[i\sqrt{5}]$ est noethérien et il vérifie la propriété **(E)**. De plus le polynôme $X^2 + 5$ est irréductible donc l'idéal $(X^2 + 5)$ est premier (proposition (iii) du 3.2) et l'anneau $\mathbb{Z}[X]/(X^2 + 5)$ est intègre. Enfin cet anneau ne vérifie pas la propriété **(U)** de l'unicité de la décomposition car $9 = 3\times3 = \left(2 + i\sqrt{5}\right)\left(2 - i\sqrt{5}\right)$ et on vérifie que 3, $2 + i\sqrt{5}$ et $2 - i\sqrt{5}$ sont irréductibles.

IV Soit $A = \mathbb{C}[X, Y]/(Y - X^2)$. Montrer que *A* est isomorphe à $\mathbb{C}[X]$ (indication : considérer le morphisme d'anneaux φ de $\mathbb{C}[X, Y]$ dans $\mathbb{C}[X]$ qui à *P* associe $P(X, X^2)$ puis sa décomposition canonique).

L'application φ de est clairement un morphisme d'anneaux surjectif. Déterminons son noyau. On a $P \in \text{Ker } \varphi$ ssi $P(X, X^2) = 0$. La division euclidienne de *P* par $Y - X^2$ donne l'existence de deux polynômes *Q* et *R* dans $\mathbb{C}[X, Y]$ tels que $P(X, Y) = (Y - X^2)Q(X, Y) + R(X, Y)$ et $d°R < 1$ (degré par rapport à *Y*). On a donc $R(X, Y) = R(X)$ et comme $P(X, X^2) = 0$ il vient $R(X) = 0$ soit $P(X, Y) = (Y - X^2)Q(X, Y)$ et Ker $\varphi \subset (Y - X^2)$ (idéal engendré par $Y - X^2$). L'inclusion réciproque étant évidente on obtient Ker $\varphi = (Y - X^2)$.

En passant φ au quotient on obtient l'isomorphisme $\overline{\varphi}$ de $\mathbb{C}[X, Y]/(Y - X^2)$ dans $\mathbb{C}[X]$ qui à $\overline{P}$ associe $P(X, X^2)$ (exercice 10).

V Montrer que $\mathbb{C}[X, Y]/(XY-1)$ est isomorphe à l'anneau $\{ \frac{P(X)}{X^n} / n \in \mathbb{N} \text{ et } P \in \mathbb{C}[X]\}$ (s'inspirer de l'exercice précédent). En utilisant l 'exercice 21 montrer que cet anneau est euclidien.

L'application φ de $\mathbb{C}[X, Y]$ dans l'anneau $A = \{ \frac{P(X)}{X^n} / n \in \mathbb{N}$ et $P \in \mathbb{C}[X]\}$ qui à $P(X, Y)$ associe $P\left(X, \frac{1}{X}\right)$ est un morphisme d'anneaux surjective (car $\varphi(P(X)Y^n) = \frac{P(X)}{X^n}$). Déterminons son noyau. Soit $P \in \text{Ker } \varphi$, donc $P\left(X, \frac{1}{X}\right) = 0$. Plaçons nous dans l'anneau $\mathbb{C}(X)[Y]$, où $\mathbb{C}(X)$ est le corps des fractions de $\mathbb{C}[X]$. Le polynôme $P(X, Y)$ s'annule pour $Y = \frac{1}{X}$, donc il est factorisable par $Y - \frac{1}{X}$: il existe $Q(X, Y) \in \mathbb{C}[X, Y]$ tel que $P(X, Y) = \left(Y - \frac{1}{X}\right)Q(X, Y)$ soit $P(X, Y) = (XY-1)\frac{Q(X,Y)}{X}$. Si on pose $P = \sum_{k\geq 0} a_k(X)Y^k$ et $Q = \sum_{k\geq 0} q_k(X)Y^k$ il vient par identification $a_0(X) = -\frac{q_0(X)}{X}$ et $a_k(X) = q_{k-1}(X) - \frac{q_k(X)}{X}$ pour $k \geq 1$ d'où $q_0(X) = -Xa_0(X)$ et $q_k(X) = X\left(q_{k-1}(X) - a_k(X)\right)$ d'où on déduit que $\frac{Q(X,Y)}{X} \in \mathbb{C}[X, Y]$. Ainsi Ker $\varphi \subset (XY-1)$, et l'inclusion réciproque étant évidente on a Ker $\varphi = (XY-1)$. En passant φ au quotient on obtient l'isomorphisme $\overline{\varphi}$ de $\mathbb{C}[X, Y]/(XY-1)$ dans A qui à $\overline{P}(X, Y)$ associe $P\left(X, \frac{1}{X}\right)$.

Si on pose $S = \{X^n / n \in \mathbb{Z}\}$ alors l'anneau A est le localisé de $\mathbb{C}[X]$ par rapport à S et $\mathbb{C}[X]$ étant euclidien il en est de même de A (exercice 21).

VI Soit $A = \mathbb{C}[X, Y]/(Y^2 - X^3)$. Montrer que A est isomorphe à l'ensemble des polynômes de $\mathbb{C}[T]$ dont le coefficient de terme en T est nul (considérer le morphisme d'anneaux φ de $\mathbb{C}[X, Y]$ dans $\mathbb{C}[T]$ qui à P associe $P(T^2, T^3)$).

Montrer que A est intègre et noethérien et donc vérifie (E) (voir III).

Montrer que A ne vérifie pas (U) (montrer que T^6 a deux décompositions).

L'application φ de $\mathbb{C}[X, Y]$ dans $\mathbb{C}[T]$ qui à $P(X, Y)$ associe $P(T^2, T^3)$. C'est clairement est un morphisme d'anneaux. Cherchons son noyau. Soit $P(X, Y) \in \text{Ker } \varphi$. La division euclidienne de P par $Y^2 - X^3$ donne $P(X, Y) = (Y^2 - X^3)Q(X, Y) + YA(X) + B(X)$ avec A et B dans $\mathbb{C}[X]$ et $Q \in \mathbb{C}[X, Y]$. Comme $P(T^2, T^3) = 0$ il vient $T^3A(T^2) + B(T^2) = 0$. En considérant les puissances paires et impaires de ce polynôme on obtient immédiatement $A = B = 0$. Ainsi Ker $\varphi = (Y^2 - X^3)$.

Déterminons maintenant l'image de φ. Si $P(X, Y) = \sum_{i,j\geq 0} a_{i,j}X^iY^j$ on a $\varphi(P) = \sum_{i,j\geq 0} a_{i,j}T^{2i+3j}$ et donc le terme en T est nul. Réciproquement si $P \in \mathbb{C}[T]$ a son terme en T nul il s'écrit $P = \sum_{k\geq 0} a_{2k}T^{2k} + \sum_{k\geq 1} a_{2k+1}T^{2k+1}$ et on a $\sum_{k\geq 0} a_{2k}T^{2k} = \varphi\left(\sum_{k\geq 0} a_{2k}X^k\right)$ et $\sum_{k\geq 1} a_{2k+1}T^{2(k-1)+3} = \varphi\left(\sum_{k\geq 1} a_{2k+1}X^{k-1}Y\right)$ donc Im $\varphi = \{\sum_{k\geq 0} a_kT^k / a_1 = 0\}$.

En passant φ au quotient on obtient un isomorphisme de $\mathbb{C}[X, Y]/(Y^2 - X^3)$ dans Im φ et on peut donc identifier A et Im φ.

Im φ est intègre car inclus dans l'anneau intègre $\mathbb{C}[T]$ et par conséquent A est intègre.

D'après III/ b/ l'anneau A est noethérien donc il vérifie la propriété **(E)**.

Or A ne vérifie pas la propriété **(U)** car on a $T^6 = T^3T^3 = T^2T^2T^2$ et comme T n'appartient pas à Im φ, T^2 et T^3 sont irréductibles.

VII *Carrés d'un corps*

Soit F_q le corps (unique à un isomorphisme près) à $q = p^n$ éléments (voir cours) avec p premier et $n \in \mathbb{N}^*$. On pose :

$$F_q^2 = \{x \in F_q \,/\, \exists\, y \in F_q \text{ tel que } x = y^2\} \text{ et } F_q^{2*} = F_q^2 - \{0\}.$$

a/ Si $p = 2$ montrer que $F_q^2 = F_q$ (considérer l'homomorphisme de Fröbenius).

b/ Si $p > 2$ montrer que $|F_q^2| = \dfrac{q+1}{2}$ et $|F_q^{2*}| = \dfrac{q-1}{2}$ (considérer l'homomorphisme de groupes de F_q^2 dans F_q^2 qui à x associe x^2).

c/ En déduire que si $p > 2$ on a : $x \in F_q^{2*} \Leftrightarrow x^{\frac{q-1}{2}} = 1$, puis que :

$$-1 \in F_q^{2*} \Leftrightarrow q \equiv 1\ (4).$$

d/ Montrer qu'il y-a une infinité de nombres premiers de la forme $1 + 4k$ ($k \in \mathbb{N}$).

(Raisonner par l'absurde : s'il n'en existe qu'un nombre fini soit n le plus grand d'entre eux et p un nombre premier divisant $(n!)^2 + 1$; on a $p \geq n + 1$ et dans $\mathbb{Z}/p\mathbb{Z}$: $(n!)^2 = -1$; donc -1 est un carré et donc $p \equiv 1\ (4)$).

a/ Si $p = 2$ on a $q = 2^n$; soit l'homomorphisme de Fröbenius $x \mapsto x^2$. C'est un isomorphisme de corps de F_q dans lui-même d'après l'exercice 14, donc $F_q^2 = F_q$.

b/ Soit φ l'homomorphisme injectif de groupes multiplicatifs de F_q^* dans F_q^{2*} qui à x associe x^2 (c'est bien un homomorphisme F_q étant commutatif car fini). Cherchons son noyau : on a $x \in \text{Ker}\ \varphi$ ssi $x^2 = 1$, soit $(x-1)(x+1) = 0$, soit $x = \pm 1$. Comme $p \neq 2$on a $1 \neq -1$ donc Ker φ a deux éléments. En passant φ au quotient on obtient un isomorphisme de groupes de $F_q^*/\text{Ker}\ \varphi$ dans F_q^{2*} donc Card F_q^{2*} = Card $F_q^*/2 = \dfrac{q-1}{2}$. Comme $F_q^{2*} = F_q^2 \cup \{0\}$ on a Card $F_q^2 = \dfrac{q-1}{2} + 1 = \dfrac{q+1}{2}$.

c/ Soit $x \in F_q^{2*}$. Il existe $y \in F_q^*$ tel que $x = y^2$, donc $x^{\frac{q-1}{2}} = y^{q-1} = 1$ (le groupe multiplicatif F_q^* ayant $q-1$ éléments), donc tout élément de F_q^{2*} est solution de l'équation polynomiale $X^{\frac{q-1}{2}} = 1$. Or cette équation a au plus $\dfrac{q-1}{2}$ solutions et Card $F_q^{2*} = \dfrac{q-1}{2}$ donc F_q^{2*} est l'ensemble des solutions de cette équation. On a donc $x \in F_q^{2*} \Leftrightarrow x^{\frac{q-1}{2}} = 1$.

On a donc : $-\overline{1} \in F_q^{2*} \Leftrightarrow \left(-\overline{1}\right)^{\frac{q-1}{2}} = \overline{1} \Leftrightarrow \dfrac{q-1}{2}$ pair $\Leftrightarrow q \equiv 1\ (4)$.

d/ Supposons que l'ensemble des nombres premiers de la forme $1 + 4k$ ($k \in \mathbb{N}$) soit fini. Soit n le plus grand de ces nombres. Soit p un nombre premier divisant $(n!)^2 + 1$. On a $p > n$ (sinon p divise $(n!)^2$, donc p divise 1), et modulo p on a : $\overline{(n!)^2 + 1} = \overline{0}$, soit $\overline{(n!)^2} = -\overline{1}$, donc p est un nombre premier de la forme $1 + 4k$ d'après 2/ ce qui est impossible car $p > n$.

VIII *Anneau de Gauss; somme de deux carrés*

Soit $A = \mathbb{Z}[i] = \{a + ib \,/\, a \text{ et } b \in \mathbb{Z}\}$.

a/ Montrer que A est un anneau commutatif, intègre, isomorphe à $\mathbb{Z}[X]/(X^2 + 1)$ (considérer le morphisme d'anneaux $P \mapsto P(i)$ de $\mathbb{Z}[X]$ dans A).

b/ Montrer que $z = a + ib \mapsto a - ib$ est un automorphisme d'anneau de A.

c/ Soit N l'application $z \mapsto z\bar{z} = a^2 + b^2$ de A dans $\mathbb{N}$. Montrer que pour tous z et z' de A on a : $N(zz') = N(z)N(z')$ et que $N(z) = 0 \Leftrightarrow z = 0$.

d/ Précisez A^*, groupe des éléments inversibles de A.

e/ Montrer que : $\forall\ z \in A$, $\forall\ t \in A-\{0\}$, $\exists q \in A$ et $\exists\ r \in A$ tels que $z = tq + r$ et $N(r) < N(t)$.

En déduire que A est euclidien (donc principal).

On pose $\Sigma = \{n \in \mathbb{N} / \exists (a, b) \in \mathbb{N}\times\mathbb{N}$ avec $n = a^2 + b^2\}$.

f/ Montrer que si $n \equiv 3$ (4) alors $n \notin \Sigma$ (<u>indication</u> : un carré est congru à 0 ou 1 modulo 4).

g/ Montrer que Σ est stable par multiplication.

h/ Si p est un nombre premier, montrer que : $p \in \Sigma \Leftrightarrow p \equiv 1$ (4)

(<u>indication</u> : montrer d'abord que : $p \in \Sigma \Leftrightarrow p$ non irréductible dans $\mathbb{Z}[i]$ puis raisonner ensuite dans $\mathbb{Z}[i]/(p)$ isomorphe à $(\mathbb{Z}/p\mathbb{Z})[X]/(X^2 + 1)$ en utilisant VII).

i/ En déduire que si $n \in \mathbb{N}-\{0, 1\}$ et $n = \prod_{p\in P} p^{v_p(n)}$ sa décomposition en produit de facteurs premiers on a :

$n \in \Sigma \Leftrightarrow v_p(n)$ est pair pour $p \equiv 3$ (4).

a/ On montre facilement que $A = \mathbb{Z}[i]$ est un sous-anneau intègre de $\mathbb{C}$. D'autre part l'application φ de $\mathbb{Z}[X]$ dans $\mathbb{C}$ qui à P associe $P(i)$ est un morphisme surjectif d'anneaux. Soit $P \in \mathbb{Z}[X]$; on écrit $P = (X^2 + 1)Q + aX + b$ avec $Q \in \mathbb{Z}[X]$ et $(a, b) \in \mathbb{Z}^2$ (division euclidienne de P par $X^2 + 1$) et on a $P \in \text{Ker}\ \varphi$ ssi $P(i) = 0$ ssi $ai + b = 0$ ssi $a = b = 0$. Ainsi Ker $\varphi = (X^2 + 1)Q$ et en passant φ au quotient on obtient un isomorphisme de $\mathbb{Z}[X]/(X^2 + 1)$ dans A.

b/ Vérification facile.

c/ Pour z et z' dans A on a $N(zz') = |zz'|^2 = |z|^2.|z'|^2 = N(z).N(z')$, et $N(z) = 0$ ssi $|z| = 0$ ssi $z = 0$.

d/ Soit $z \in A$ inversible dans A. Il existe $z' \in A$ tel que $zz' = 1$, donc $N(zz') = 1$, soit $N(z)N(z') = 1$ d'où $N(z) = 1$ (car $N(z)$ et $N(z')$ appartiennent à $\mathbb{N}$). Si $z = a + ib$ ($(a; b) \in \mathbb{Z}^2$) on obtient $a^2 + b^2 = 1$, soit $a = \pm 1$ et $b = \pm 1$. Comme ± 1 et $\pm i$ sont inversibles dans A on a $A^* = \{-1, 1, -i, i\}$.

e/ Prouvons d'abord le lemme : soit $z \in \mathbb{C}^*$; il existe $\alpha \in A$ tel que $|z - \alpha| < 1$. En effet si $z = x + iy$, soient a et b des entiers relatifs les plus proches de x et y. On a $|x - a| \le 1/2$ et $|y - b| \le 1/2$, d'où $|z - (a + ib)|^2 = (x - a)^2 + (y - b)^2 \le (1/2)^2 + (1/2)^2 = 1/2$, soit $|z - \alpha| \le \sqrt{2}/2 < 1$ avec $\alpha = a + ib$.

Soient maintenant $z \in A$ et $t \in A-\{0\}$. D'après le lemme il existe $q \in A$ tel que $|z/t - q| < 1$, soit $|z - qt| < |t|$. En posant $r = z - tq$ on aura $z = tq + r$ et $N(r) < N(t)$. Il en résulte que A est un anneau euclidien (avec $v = N$).

f/ Un carré étant congru à 0 ou 1 modulo 4 on a $a^2 + b^2 \equiv 0, 1$ ou 2 (4). Donc si $n \equiv 3$ (4) alors $n \notin \Sigma$.

g/ Soient $n = a^2 + b^2$ et $m = c^2 + d^2$ appartenant à Σ (avec a, b, c et d dans $\mathbb{N}$). On a $(a + ib)(c + id) = (ac - bd) + i(ad + bc)$ et en prenant le carré du module des deux membres il vient $mn = (a^2 + b^2)(c^2 + d^2)$

$= (ac - bd)^2 + (ad + bc)^2$, donc $mn \in \Sigma$.

h/ Soit p un nombre premier. Si $p \in \Sigma$ alors $p = a^2 + b^2$ (a et b dans $\mathbb{N}$), donc $p = (a + ib)(a - ib)$ et $N(a + ib) = N(a - ib) = p > 1$, donc $a + ib$ et $a - ib$ ne sont pas inversibles donc p n'est pas irréductible dans A. Réciproquement si p n'est pas irréductible dans A, il existe u et v non inversibles dans A tels que $p = u.v$, donc $p^2 = N(u)N(v)$. Comme u et v sont irréductibles dans A on a $N(u)$ et $N(v) > 1$, donc, p étant premier, on a $p = N(u) = N(v)$ et p appartient à Σ.

On a donc : $p \in \Sigma \Leftrightarrow p$ non irréductible dans $A = \mathbb{Z}[i] \Leftrightarrow$ l'idéal (p) non premier dans A (car A est principal) $\Leftrightarrow$ $\mathbb{Z}[X]/(X^2 + 1)/(p)$ non intègre $\Leftrightarrow (\mathbb{Z}/p\mathbb{Z})[X]/(X^2 + 1)$ non intègre $\Leftrightarrow X^2 + 1$ non irréductible dans $(\mathbb{Z}/p\mathbb{Z})[X] \Leftrightarrow$ $X^2 + 1$ a au moins une racine dans $\mathbb{Z}/p\mathbb{Z} \Leftrightarrow -1$ est un carré dans le corps $\mathbb{Z}/p\mathbb{Z} \Leftrightarrow p \equiv 1$ (4) (d'après VII/).

i/ Si $v_p(n)$ est pair pour $p \equiv 3$ (4) il est clair que $n \in \Sigma$ d'après g/ et h/.

Réciproquement soit p un nombre premier congru à 3 modulo 4 considérons pour m appartenant à $\mathbb{N}$ la propriété $P(m)$: "$\forall\ n \in \Sigma$, $v_p(n)$ est pair $v_p(n) \le m$". Montrons par récurrence m cette propriété. $P(0)$ est vraie. Supposons la propriété $P(k)$ vraie pour $k \le m$ et soit n appartenant à Σ tel que $v_p(n) = m + 1$. On a $v_p(n) > 0$ donc p divise $n = a^2 + b^2 = (a + ib)(a - ib)$. Or p est irréductible dans A d'après h/ donc p divise $a + ib$ ou p divise $a - ib$ (lemme d'Euclide). Si p divise $a + ib$ alors $a + ib = p.u$ (avec $u \in A$) donc $a^2 + b^2 = p^2.N(u)$, donc p^2 divise $n = a^2 + b^2$ et

$n/p^2 = N(u) \in \Sigma$. Comme $v_p(n/p^2) = v_p(n) - 2 \leq m$, d'après l'hypothèse de récurrence $v_p(n) - 2$ est pair donc $v_p(n)$ aussi ce qui achève la récurrence.

IX *Anneau* $\mathbb{Z}[\sqrt{2}]$

On pose $\mathbb{Q}[\sqrt{2}] = \{r + r'\sqrt{2} \ / \ r \text{ et } r \in \mathbb{Q}\}$.

1°/ Soit N l'application de $\mathbb{Q}[\sqrt{2}]$ dans $\mathbb{R}$ qui à $z = r + r'\sqrt{2}$ (r et r' dans $\mathbb{Q}$) associe $N(z) = |r^2 - 2r'^2|$. Montrer que cette application est bien définie et que pour tous z et z' de A on a : $N(zz') = N(z)N(z')$, $N(z/z') = N(z)/N(z')$ (si $z' \neq 0$) et ($N(z) = 0 \Leftrightarrow z = 0$).

2°/ Montrer que $\mathbb{Q}[\sqrt{2}]$ est un sous-corps de $\mathbb{R}$.

On pose $A = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \ / \ a \text{ et } b \in \mathbb{Z}\}$.

3°/ Montrer que A est un anneau commutatif, intègre, isomorphe à $\mathbb{Z}[X]/(X^2 - 2)$ (s'inspirer du V).

4°/ Montrer que pour tout $x \in A$ et tout $y \in A - \{0\}$ il existe $(q, r) \in A \times A$ tel que :

$x = yq + r$ avec $N(r) < N(y)$.

(<u>indication</u> : déterminer $q \in A$ tel que $N\left(\frac{x}{y} - q\right) < 1$).

A est donc un anneau euclidien. Le couple (q, r)est-il unique ?

5°/ Le but de la question est de déterminer A^*, ensemble des éléments inversibles de A.

a/ Montrer que $z \in A^* \Leftrightarrow N(z) = 1$.

On pose $J = \{x \in A^* / \ x > 0\}$ et $K = \{x \in A^* / \ x > 1\}$

b/ Montrer que $K = \{a + b\sqrt{2} \in A^* / \ a \text{ et } b \in \mathbb{N}^*\}$. Montrer que le minimum de K est $1 + \sqrt{2}$.

c/ Montrer que $K = \{(1 + \sqrt{2})^n / \ n \in \mathbb{N}\}$ (<u>indication</u> : si $x \in K$ considérer l'entier naturel n tel que $(1 + \sqrt{2})^n \leq x < (1 + \sqrt{2})^{n+1}$; si l'inégalité est stricte aboutir à une contradiction en divisant par $(1 + \sqrt{2})^n$).

d/ En déduire enfin que $J = \{(1 + \sqrt{2})^n / \ n \in \mathbb{Z}\}$ puis que $A^* = \{\pm(1 + \sqrt{2})^n / \ n \in \mathbb{Z}\}$.

e/ <u>Application</u> : résoudre dans $\mathbb{Z} \times \mathbb{Z}$ les équations :

(i) $x^2 - 2y^2 = 1$;

(ii) $x^2 - 2y^2 = -1$.

1°/ Montrons d'abord que pour tout z appartenant à $\mathbb{Q}[\sqrt{2}]$ il existe un couple unique (r, r') de rationnels tel que $z = r + r'\sqrt{2}$. En effet si $= r + r'\sqrt{2} = = \rho + \rho'\sqrt{2}$ avec r, r', ρ et ρ' appartenant $\mathbb{Q}$, on en déduit, si $r' \neq \rho'$, $\sqrt{2} = \frac{r - \rho}{\rho' - r'}$, ce qui est impossible car $\sqrt{2}$ n'est pas rationnel, donc $r' = \rho'$, puis $r = \rho$. L'application N est donc bien définie. Si on pose $\overline{z} = r - r'\sqrt{2}$ (pour $z = r + r'\sqrt{2}$) alors $N(z) = |z.\ \overline{z}|$ d'où il résulte que $N(z.z') = N(z).N(z')$ pour tous z et z' de $\mathbb{Q}[\sqrt{2}]$.

D'autre part, si $N(z) = 0$ (avec $z = r + r'\sqrt{2}$), on a $r^2 - 2r'^2 = 0$, et si $r' \neq 0$ on en déduit $2 = r^2/r'^2$ ce qui est absurde car $\sqrt{2}$ est irrationnel. On a donc $r' = 0$, d'où $r = 0$. On a donc, pour tout z de $\mathbb{Q}[\sqrt{2}]$, $N(z) = 0$ ssi $z = 0$.

Si $z = r + r'\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ est non nul on donc $N(z) = N(\overline{z}) = |r^2 - 2r'^2| \neq 0$ donc $\overline{z} \neq 0$ et $\frac{1}{z} = \frac{1}{r - r'\sqrt{2}} = \frac{r + r'\sqrt{2}}{r^2 - 2r'^2} = \overline{\left(\frac{1}{z}\right)}$, d'où $N\left(\frac{1}{z}\right) = \left|\frac{1}{z}.\overline{\left(\frac{1}{z}\right)}\right| = \left|\frac{1}{z}.\frac{1}{\overline{z}}\right| = \frac{1}{|z.\overline{z}|} = \frac{1}{N(z)}$. Il en résulte, avec la relation $N(z.z') = N(z).N(z')$, que $N(z/z') = N(z)/N(z')$ pour $z \in \mathbb{Q}[\sqrt{2}]$ et $z' \in \mathbb{Q}[\sqrt{2}] - \{0\}$.

2°/ On montre facilement que $\mathbb{Q}[\sqrt{2}\,]$ est un sous-anneau de $\mathbb{R}$. De plus si $z = r + r'\sqrt{2} \in \mathbb{Q}[\sqrt{2}\,] - \{0\}$, alors $N(z) = |r^2 - 2r'^2| \neq 0$ et $\frac{1}{z} = \frac{1}{r + r'\sqrt{2}} = \frac{r - r'\sqrt{2}}{r^2 - 2r'^2} \in \mathbb{Q}[\sqrt{2}\,]$, donc $\mathbb{Q}[\sqrt{2}\,]$ est un sous-corps de $\mathbb{R}$.

3°/ On vérifie facilement que A est un sous-anneau de $\mathbb{R}$. Comme dans l'exercice précédent, on considère le morphisme d'anneaux surjectif φ de $\mathbb{Z}[X]$ dans A qui à P associe $P(\sqrt{2}\,)$. En écrivant

$P = (X^2 - 2)\,Q + aX + b$ avec $Q \in \mathbb{Z}[X]$ et $(a, b) \in \mathbb{Z}^2$ (division euclidienne de P par $X^2 - 2$) on montre que Ker $\varphi = (X^2 - 2)$ (idéal engendré par $X^2 - 2$) et en passant φ au quotient on obtient un isomorphisme de $\mathbb{Z}[X]/(X^2 - 2)$ dans A.

4°/ On procède comme à l'exercice précédent : si $z = X + Y\sqrt{2}$ (avec X et Y rationnels), soient a et b des entiers relatifs les plus proches de X et Y. On a $|X - a| \leq 1/2$ et $|Y - b| \leq 1/2$, d'où $N(z - (a + b\sqrt{2}\,)) = |(X - a)^2 - 2(Y - b)^2| \leq (1/2)^2 + 2.(1/2)^2 = 3/4$, soit $N(z - q) < 3/4 < 1$ avec $q = a + b\sqrt{2} \in A$. Il en résulte que si $x \in A$ et $y \in A - \{0\}$, il existe $q \in A$ tel que $N\left(\frac{x}{y} - q\right) < 1$, soit $N\left(\frac{x - qy}{y}\right) = \frac{N(x - qy)}{N(y)} < 1$ ou $N(x - yq) < N(y)$. Si on pose $r = x - yq$, on a $x = yq + r$ et $N(r) < N(y)$.

Le couple (q, r) n'est pas unique : par exemple pour $x = 1/2$ et $y = 1$ les couples $(1/2, 0)$ et $(0, 1/2)$ conviennent.

5°/ a/ Si $z \in A^*$, il existe z' dans A tel que $z.z' = 1$. Donc $N(z.z') = N(1) = 1$, soit $N(z) = 1$ (car $N(z)$ et $N(z')$ appartiennent à $\mathbb{N}$).

Réciproquement si $N(z) = 1$ avec $z \in A$, alors $z.\overline{z} = 1$, et comme $\overline{z} \in A$, z est inversible dans A.

b/ On a clairement $\{a + b\sqrt{2} \in A^*/\ a \text{ et } b \in \mathbb{N}^*\} \subset K$. Réciproquement soit $x \in K$. Il existe $(a, b) \in \mathbb{Z}^2$ tel que $x = a + b\sqrt{2}$ et d'après 5/ a/ $N(x) = 1$, donc $|a^2 - 2b^2| = 1$. Clairement a et b sont non nuls (si $a = 0$ alors $2b^2 = 1$, impossible et si $b = 0$ alors $a^2 = 1$, donc $a = 1$, impossible car $x > 1$). Supposons $a < 0$ et $b > 0$. On a $(a + b\sqrt{2}\,).(-a + b\sqrt{2}\,) = |a^2 - 2b^2| = 1$. Or $a + b\sqrt{2} > 1$(car $x \in K$) et $-a + b\sqrt{2} > 1$ (car $-a$ et b appartiennent à $\mathbb{N}^*$), d'où absurdité. Si $a > 0$ et $b < 0$ on a de même $(a + b\sqrt{2}\,).(a - b\sqrt{2}\,) = |a^2 - 2b^2| = 1$ et c'est aussi impossible car $a + b\sqrt{2}$ et $a - b\sqrt{2}$ sont tous deux strictement supérieurs à 1. on a donc a et b strictement positifs donc $K = \{a + b\sqrt{2} \in A^*/\ a \text{ et } b \in \mathbb{N}^*\}$.

Pour tout x dans K on a donc $x \geq 1 + \sqrt{2}$. Comme $1 + \sqrt{2} \in K$(car $N(1 + \sqrt{2}\,) = 1$) on a $1 + \sqrt{2} = \text{Min } K$.

c/ Comme $1 + \sqrt{2}$ est inversible alors $(1 + \sqrt{2}\,)^n$ aussi pour tout entier naturel n et est > 1 donc $(1 + \sqrt{2}\,)^n \in K$ soit $\{(1 + \sqrt{2}\,)^n / n \in \mathbb{N}\} \subset K$.

Réciproquement soit $x \in K$. Soit l'entier naturel n tel que $(1 + \sqrt{2}\,)^n \leq x < (1 + \sqrt{2}\,)^{n+1}$ (n existe car $x > 1$ et la suite $(1 + \sqrt{2}\,)^n$ tend vers l'infini). Si $(1 + \sqrt{2}\,)^n < x < (1 + \sqrt{2}\,)^{n+1}$ alors on aurait $1 < \frac{x}{\left(1+\sqrt{2}\right)^n} < 1 + \sqrt{2}$. Or x et $(1 + \sqrt{2}\,)^n$ sont inversibles donc $\frac{x}{\left(1+\sqrt{2}\right)^n}$ aussi donc on aurait $\frac{x}{\left(1+\sqrt{2}\right)^n} \in K$ et $\frac{x}{\left(1+\sqrt{2}\right)^n} < 1$ ce qui est impossible car $1 + \sqrt{2} = \text{Min } K$. On a donc $x = (1 + \sqrt{2}\,)^n$ et ainsi $K = \{(1 + \sqrt{2}\,)^n / n \in \mathbb{N}\}$.

d/ Si $n \in \mathbb{Z}$ on a $(1 + \sqrt{2}\,)^n$ inversible et > 0 donc c'est un élément de J donc $\{(1 + \sqrt{2}\,)^n / n \in \mathbb{Z}\} \subset J$.

Réciproquement soit $x \in J$, distinct de 1. Si $x > 1$ alors $x \in K$ donc x s'écrit $(a + b\sqrt{2}\,)^n$ avec n, a et b dans $\mathbb{N}$. Si $0 < x < 1$, alors $1/x$ est inversible dans A et > 1, donc on a de même $1/x = (a + b\sqrt{2}\,)^n$ avec n, a et b dans $\mathbb{N}$, soit $x = (a + b\sqrt{2}\,)^{-n}$. Finalement on a bien $J = \{(1 + \sqrt{2}\,)^n / n \in \mathbb{Z}\}$.

D'autre par on a $x \in A^*$ ssi x ou $-x$ appartient à J donc $A^* = \{\pm(1 + \sqrt{2}\,)^n / n \in \mathbb{Z}\}$.

e/ si $(x, y) \in \mathbb{Z}^2$ vérifient $x^2 - 2y^2 = \pm 1$, alors $z = x + y\sqrt{2} \in A^*$, donc $z = \pm(1 + \sqrt{2})^n$ (avec $n \in \mathbb{Z}$). Réciproquement si $x + y\sqrt{2} = \pm(1 + \sqrt{2})^n$, on a $x^2 - 2y^2 = \left(1+\sqrt{2}\right)^n . \overline{\left(1+\sqrt{2}\right)^n} = \left[\left(1+\sqrt{2}\right).\overline{\left(1+\sqrt{2}\right)}\right]^n = (-1)^n$.

Les solutions de (i) sont donc les couples $(x, y) \in \mathbb{Z}^2$ avec $x + y\sqrt{2} = \pm(1 + \sqrt{2})^n$ et n pair, et les solutions de (ii) sont donc les couples $(x, y) \in \mathbb{Z}^2$ avec $x + y\sqrt{2} = \pm(1 + \sqrt{2})^n$ et n impair.

X Soit A un anneau commutatif. A quelle condition nécessaire et suffisante sur A est-il vrai que pour tout entier naturel non nul n, tout polynôme de $A[X]$ de degré n admet n racines au plus ?

(Réponse : A est intègre; si A n'est pas intègre et si a et b sont des diviseurs de 0, considérer le polynôme $(X - a)(X - b)$).

Si A est intègre on le plonge dans son corps des fractions K. Dans $K[X]$ tout polynôme de degré n non nul à au plus n racines donc le résultat est vrai aussi dans $A[X]$.

Réciproquement si A n'est pas intègre il existe deux éléments a et b non nuls tels que $a.b = 0$. Si $a \neq b$ alors le polynôme $(X - a)(X - b)$ a pour racines a, b et 0. Si $a = b$ on a $a^2 = 0$ et le polynôme $(X - a)^2 = X^2 - 2aX$ a pour racines a, $2a$ et 0.

XI *Critère d'irréductibilité d'Eisenstein*

Soit A un anneau factoriel, K son corps des fractions et $P(X) = a_n X^n + ... + a_0 \in A[X]$. On suppose qu'il existe un élément irréductible p de A tel que :

(i) p ne divise pas a_n;

(ii) $\forall\ i \in \{0, 1, ... , n - 1\}$, p divise a_i;

(iii) p^2 ne divise pas a_0.

Montrer que P est irréductible dans $K[X]$ (donc dans $A[X]$ si pgcd$(a_i) = 1$).

Applications :

Si p est premier, $X^{p-1} + X^{p-2} ... + X + 1$ est irréductible dans $\mathbb{Z}[X]$;

$X^4 + 1$ est irréductible dans $\mathbb{Z}[X]$ (poser $X = Y + 1$).

On écrit $P = u\sum_{k=0}^{n} \alpha_k X^k$, u étant un pgcd des coefficients $a_0, \ldots, a_n$ de P. Comme p ne divise pas a_n alors p ne divise pas u. D'après le lemme d'Euclide, comme p divise $a_0, \ldots, a_n$ alors p divise $\alpha_0, \ldots, \alpha_n$ et p^2 ne divise pas α_0. Comme u est inversible dans K on peut donc se ramener au cas où $u = 1$. Supposons que P ne soit pas irréductible dans $K[X]$ donc dans $A[X]$ (3.2, lemme 2 du théorème de Gauss). Il existe alors deux éléments $\sum_{k=0}^{\beta} b_k X^k$ et $\sum_{k=0}^{\gamma} c_k X^k$ de $A[X]$ tels que $P(X) = \sum_{k=0}^{\beta} b_k X^k . \sum_{k=0}^{\gamma} c_k X^k$ avec $\beta > 0$, $\gamma > 0$, $\beta + \gamma = n$ et $a_k = \sum_{i=0}^{k} b_i c_{k-i}$.

On a $u.a_0 = b_0 c_0$. Comme p divise a_0 alors p divise $b_0 c_0$ donc p divise b_0 ou p divise c_0. Si par exemple p divise b_0 alors p ne divise par c_0 car p^2 ne divise pas a_0.

Posons $m = \text{Max}\{k / p \text{ divise } b_0, b_1, \ldots , b_k\}$.

Supposons que $m < \beta$. On a $a_{m+1} = b_{m+1}c_0 + b_m c_1 + b_{m-1} c_2 + \ldots + b_0 c_{m+1}$. On a $m + 1 \leq \beta < n$ donc p divise a_{m+1} (hypothèse (ii)) et p divise $b_0, b_1, \ldots , b_m$ donc p divise $b_{m+1}c_0$. Comme p ne divise pas c_0 alors p divise b_{m+1} ce qui est contraire à la définition de m. Ainsi $m = \beta$ et p divise $b_0, b_1, \ldots , b_\alpha$. Or $a_n = b_\alpha c_\gamma$ donc p divise a_n ce qui contredit l'hypothèse (i).

Applications : Posons $X = Y + 1$. Comme $(X - 1)(X^{p-1} + X^{p-2} + \ldots + 1) = X^p - 1$, alors

$X^{p-1} + X^{p-2} + \ldots + 1 = \dfrac{(Y+1)^p - 1}{Y} = \sum_{i=1}^{p}\binom{p}{i}Y^{i-1}$. Comme p est premier p divise $\binom{p}{i}$ pour $1 \le i \le p-1$, et p^2 ne divise pas $\binom{p}{1} = p$, donc le polynôme $\sum_{i=1}^{p}\binom{p}{i}Y^{i-1}$ est irréductible dans $\mathbb{Q}[Y]$ et donc dans $\mathbb{Z}[Y]$ car les coefficients sont premiers entre eux. Il en résulte immédiatement que $X^{p-1} + X^{p-2} + \ldots + 1$ est irréductible dans $\mathbb{Z}[X]$.

De même en posant $X = Y + 1$ on a $X^4 + 1 = 2 + 4Y + 6Y^2 + 4Y^3 + Y^4$, et les conditions (i), (ii) et (iii) sont satisfaites avec $p = 2$.

XII Résultant de deux polynômes

1°/ CN : si P et Q ne sont pas premiers entres eux il ont un diviseur commun R de degré ≥ 1, donc il existe deux polynômes P_1 et Q_1 tels que $P = P_1R$ et $Q = Q_1R$. Alors $PQ_1 - QP_1 = 0$ et d°$Q1 \le q - 1$ et d°$P1 \le p - 1$.

CS : supposons que A et B existent et que P et Q soient premiers entre eux. Comme $AP = -BQ$, P divise BQ donc d'après le théorème de Gauss P divise B ce qui est absurde car d°$B \le p-1$ et B non nul.

2°/ Le (i) et le (ii) résultent immédiatement des propriétés des déterminants.

(a) ⇔ (b) : P et Q ne sont premiers entre eux ssi il existe d'après 1°/ deux polynômes non nuls A et B tels que d°$A \le q - 1$, d°$B \le p-1$ et $AP + BQ = 0$, i.e. $\Phi_{P,Q}(A, B) = 0$ ou $\Phi_{P,Q}$ n'est pas injective ce qui équivaut à res$(P, Q) = 0$.

3°/ a/ Pour $0 \le i \le p-1$ effectuons la division euclidienne de $X^iQ(X)$ par $P(X)$: il existe deux polynôme S_i et R_i tels que $X^iQ(X) = S_i(X)P(X) + R_i(X)$ avec d°$R_i < p$ d'où $\Psi_Q(\overline{Q(X)X^i}) = R_i(x)$. La matrice de Ψ_Q dans la base $\boldsymbol{b}$ est donc est celle du système $(R_0, R_1, \ldots, R_{p-1})$ dans la base $(1, X, \ldots, X^{p-1})$.

D'autre part on a : res$(P, Q) = \det(PX^{q-1}, \ldots, P, QX^{p-1}, \ldots, Q)$ (dans la base $(X^{p+p-1}, \ldots, 1)$). Par combinaison linéaire de colonnes on a res$(P, Q) = \det(PX^{q-1}, \ldots, P, R_{p-1}, \ldots, R_0)$. Par suite on a :

$$\text{res}(P, Q) = \begin{vmatrix} A & 0 \\ C & B \end{vmatrix}$$, où A est une matrice triangulaire inférieure dont les éléments diagonaux valent a_P et B est la matrice de Ψ_Q dans la base $\boldsymbol{b}$. On a donc : res$(P, Q) = a_p^q \det(\Psi_Q)$.

b/ (i) Si $P = X - \alpha$ le reste de la division euclidienne d'un polynôme U par P est $U(\alpha)$ donc le classe de U dans $K[X]/(P)$ est $U(\alpha)$ et Ψ_Q est définie par $\Psi_Q(U) = Q(\alpha)U(\alpha)$. Le déterminant de Ψ_Q dans la base $\boldsymbol{b}$ est donc $Q(\alpha)$ d'où le (i) d'après la propriété précédente.

(ii) Résulte du fait que $\Psi_{QR} = \Psi_Q \circ \Psi_R$ et de la propriété du 3/ a/.

(iii) On a d'après les propriétés précédentes :

$$\text{res}(P, Q) = (-1)^{pq}\text{res}(Q, P) = (-1)^{pq}\text{res}(Q, a_p\prod_{i=1}^{p}(X - \alpha_i)) =$$

$$a_p^q(-1)^{pq}\prod_{i=}^{p}\text{res}(Q, X - \alpha_i) = a_p^q(-1)^{pq}(-1)^{pq}\prod_{i=}^{p}\text{res}(X - \alpha_i, Q) = a_p^q\prod_{i=}^{p}Q(\alpha_i)$$

d'où le (iii).

On en déduit facilement la dernière formule.

4°/ Résulte facilement de la continuité du résultant de deux polynômes.

XIII

1°/ Comme $\varphi(d) \ne 0$ la condition suffisante est évidente.

Supposons $\Gamma_d \ne \varnothing$ et soit $x \in \Gamma_d$. x engendre un groupe $\langle x \rangle$ de cardinal d et tout élément y de $\langle x \rangle$ vérifie $y^d = 1$ (voir chapitre "Groupes"). Or dans un corps le polynôme $X^d - 1$ a au plus d racines; comme tout élément de $\langle x \rangle$ est racine

de ce polynôme les éléments de $<x>$ sont exactement les racines de ce polynôme, soit $<x> = E_d$. Ainsi E_d est l'unique sous-groupe cyclique de G d'ordre d (isomorphe à $\mathbb{Z}/d\mathbb{Z}$). Les éléments de Γ_d sont donc les générateurs de ce sous-groupe et ils sont au nombre de $\varphi(d)$ (en effet un élément $\overline{x} \in \mathbb{Z}/d\mathbb{Z}$ avec $0 \leq x \leq d-1$ engendre $\mathbb{Z}/d\mathbb{Z}$ ssi x est premier avec d). Donc $|\Gamma_d| = \varphi(d)$.

2°/ Si x est un élément de G sont ordre est un diviseur de n donc x appartient à un Γ_d avec d/n d'où $G = \bigcup_{d/n} \Gamma_d$. Comme $\Gamma_d \cap \Gamma_{d'} = \varnothing$ pour $d \neq d'$ cette union est disjointe donc $|G| = \sum_{d/n} |\Gamma_d|$ soit $n = \sum_{d/n} |\Gamma_d|$.

3°/ D'autre part on a $n = \sum_{d/n} \varphi(d)$ (voir exercice complémentaire VIII). Comme $|\Gamma_d| \leq \varphi(d)$ pour tout d d'après 1/ on a nécessairement $|\Gamma_d| = \varphi(d)$ pour tout diviseur d de n, et en particulier $|\Gamma_n| = \varphi(n) \neq 0$. G possède ainsi au moins un élément d'ordre n donc G est cyclique.

Application : $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z}-\{0\}$ (car $\mathbb{Z}/p\mathbb{Z}$ est un corps pour p premier) donc $(\mathbb{Z}/p\mathbb{Z})^*$ est un groupe cyclique de cardinal $p-1$ donc isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$.

4°/ Soit $x \in G$ dont l'ordre est le ppmc μ des ordres des éléments de G. Tous les éléments du groupe $<x>$ engendré par x sont solution de $X^\mu = 1$. Le polynôme $X^\mu - 1$ ayant au plus μ racine et $<x>$ étant de cardinal μ, $<x>$ est l'ensemble des zéros de ce polynôme. Mais si $y \in G$ est d'ordre d on a $y^d = 1$ donc $y^\mu = 1$ (car μ est multiple de d). Tout élément de G est racine de $X^\mu = 1$, par conséquent $G = <x>$ et G est cyclique.