Exemples d'applications des idéaux d'un anneau commutatif unitaire

prérequis : les notions d'anneau, d'idéal premier, maximal, anneau euclidien factoriel, pgcd et ppcm

1. Un exemple de plan (version très préliminaire)

Remarques d'ordre général : le titre est suffisamment explicite pour vous dissuader de toute dissertation sur les propriétés générales des anneaux euclidiens, noethérien, principaux... Vous pouvez éventuellement commencer par un paragraphe de généralités très court en vous excusant presque de trahir le titre de la leçon.
Remarques historiques : pour résoudre des équations diophantiennes du genre de celles de Fermat $x^n + y^n = z^n$, on est tenté d'appliquer des recettes qui ont fait quelques succès notamment pour $n = 2$: factoriser puis conclure en utilisant la factorialité de $\mathbb{Z}$. Le problème est que pour factoriser on est obligé de rajouter des racines, par exemple pour Fermat de travailler dans $\mathbb{Z}[\zeta]$ où ζ est une racine primitive n-ème de l'unité. Ce faisant certes on peut factoriser mais catastrophe on perd l'unicité de la factorisation. Kummer a alors introduit la notion d'idéal et a remarqué que, pour les anneaux de Dedekind, on a une propriété de factorialité pour les idéaux, i.e. tout idéal s'écrit de manière "unique" comme produit d'idéaux premiers. Pour l'équation de Fermat avec $n = p$ premier impair, dans le cas où le nombre de classe de $\mathbb{Z}[\zeta]$ est premier avec p, il a alors réussi à prouver qu'il n'y avait pas de solutions (il utilise le principe suivant : si $\mathcal{A}$ est un idéal tel que $\mathcal{A}^p$ est principal alors $\mathcal{A}$ est principal, de sorte que l'on se retrouve comme si l'anneau était principal, cf. un exemple dans les exercices).

Les thèmes centraux de cette leçon sont :
- la résolution des équations diophantiennes ;
- le calcul formel via les bases de Gröbner ;
- la géométrie algébrique.

Cependant ses thèmes ne sont pas au programme de l'agrégation, il faudra donc proposer un plan à la mesure de ses connaissances...

I-*Généralités :*

a) - Rappelons que pour une partie I de A, les lois de A induisent une structure d'anneau sur A/I si et seulement si I est un idéal de A. En outre A/I est intègre (resp. un corps) si et seulement si I est premier (resp. maximal).
applications :
- *Construction des extensions de corps* : pour K un corps et $P(X) \in K[X]$ irréductible alors $L = K[X]/(P(X))$ est une extension de degré $\deg P$ de K. Par exemple sachant que pour tout n il existe un unique corps à isomorphisme près de cardinal p^n, celui-ci est isomorphe à $\mathbb{F}_p[X]/(P(X))$ où $P(X)$ est un polynôme irréductible de $\mathbb{F}_p[X]$ (ex : $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2 + X + 1)$).
- *Détermination des idéaux premiers* : par exemple pour $p \in \mathbb{Z}$ impair, l'idéal (p) de $\mathbb{Z}[i]$ est premier si et seulement si $\mathbb{Z}[i]/(p) \simeq \mathbb{F}_p[X]/(X^2+1)$ est intègre et donc si et seulement si $X^2 + 1$ est irréductible modulo p, i.e. $(\frac{-1}{p}) = -1$ et donc $p \equiv 3 \mod 4$. Les autres idéaux premiers sont $(1 + i)$ et $(x + iy)$ avec $x^2 + y^2 \in \mathbb{Z}$ premier.
- *Détermination des idéaux maximaux* : par exemple l'idéal $(X_1 - x_1, \cdots, X_n - x_n)$ est maximal dans $K[X_1, \cdots, X_n]$.

- Constructions usuelles sur les idéaux : $I \cap J$, $I + J$, $I : J = \{a \in A : \ ab \in I \forall b \in J\}$ et les diverses relations entre elles : par exemple $(I_1 \cap I_2) : (f) = (I_1 : f) \cap (I_2 : f)$.

b) *Anneaux principaux* : il ne s'agit pas de refaire la leçon sur les anneaux principaux mais d'insister sur quelques exemples et applications :

- pour tout corps K, $K[X]$ est euclidien et donc principal ; on définit alors le polynôme minimal
  - d'un endomorphisme ;
  - d'un entier algébrique.
- notion de pgcd et théorème de Bezout : l'idéal engendré par a et b est principal ; un générateur est alors un pgcd ; en applications, on peut citer
  - le lemme des noyaux ;
  - un sous-groupe fini de $K^\times$ est cyclique.
- résolution des équations diophantiennes simples avec par exemple
  - $n = x^2 + py^2$ pour $p = 1, 2, 3$;
  - $x^2 + y^2 = z^2$;
  - $y^2 = x^3 + 7$.
- calculs modulaires (congruences) avec par exemple
  - critère d'Eisenstein ;
  - irréductibilité des polynômes cyclotomiques ;
  - algorithme de Berlekamp et factorisation des polynômes de $\mathbb{Z}[X]$
- codes linéaires cycliques.

c) Quelques définitions autour des idéaux : nous avons déjà vu ce qu'était un idéal premier, maximal. On dit qu'un idéal est :

- *primaire* si $fg \in I$ avec $f \notin I$ alors il existe n tel que $g^n \in I$; l'exemple simple est $p^r\mathbb{Z} \subset \mathbb{Z}$ pour p premier ;
- *irréductible* s'il n'existe pas d'idéaux J_1, J_2 tels que $I = J_1 \cap J_2$ avec $I \subsetneq J_i$;
- *radical* si $f^n \in I$ implique $f \in I$.

- Un anneau noethérien est un anneau dans lequel tout idéal est de type fini (ou de manière équivalente si toute suite croissante d'idéaux est stationnaire). Le résultat fondamental est le théorème de la base de Hilbert qui dit que si A est noethérien alors $A[X]$ l'est de sorte que $K[X_1, \cdots, X_n]$ est noethérien.

- Dans un anneau noethérien tout idéal est une intersection finie d'idéaux irréductibles ; par ailleurs un idéal irréductible d'un anneau noethérien est primaire.

- Le radical $\sqrt{I}$ d'un idéal I est l'ensemble des f tels qu'il existe n avec $f^n \in I$; ainsi un idéal est radical si et seulement si $I = \sqrt{I}$. Un idéal I est primaire si et seulement si $\sqrt{I}$ est premier.

d) Le problème avec les décompositions en idéaux irréductibles est que si I_1 et I_2 sont irréductibles alors $I_1 \cap I_2$ ne l'est pas. Cependant si Q_1, Q_2 sont des idéaux P-primaires, i.e. primaires avec $\sqrt{Q}_i = P$ premier, alors $Q_1 \cap Q_2$ est encore primaire.

- Une décomposition primaire $I = \bigcap_{i=1}^n Q_i$ est dite sans redondance si $\bigcap_{i \neq j} Q_i \neq I$; en particulier les idéaux premiers $P_i = \sqrt{Q}_i$ sont deux à deux distincts ; on les appelle les premiers associés. Ceux qui ne sont pas strictement contenu dans un ordre sont dits minimaux : par exemple $(x^2, xy) = (x^2, y) \cap x$ avec (x) minimal et $\sqrt{(x^2, y)} = (x, y)$ non ; géométriquement $V(x, y)$ est l'origine tandis que $V(x)$ est la droite $x = 0$.

Lemme : soit Q un idéal P-primaire et $f \in A$ alors

- $f \in Q \Rightarrow Q : f = A$;

– $f \notin Q \Rightarrow Q : f$ est P-primaire ;
– $f \notin P \Rightarrow Q : f = Q$.

On en déduit alors que les idéaux premiers associés d'un idéal sont indépendants de la décomposition primaire.

II- *Quelques anneaux de fonctions*

a) Soit E un espace compact et $A = \mathcal{C}(E)$ l'ensemble des fonctions réelles continues sur E, muni de la topologie de la convergence uniforme.
– $A^\times$ est constitué des fonctions qui ne s'annulent jamais ;
– tout idéal maximal de A est fermé.

Soit ϕ l'application qui à un fermé associe l'idéal $V(F) = \{f \in A,\ f_{|F} = 0\}$.
– les idéaux maximaux de A sont les $V(\{a\})$ avec $a \in E$;
– ϕ établit une bijection entre les fermés de E et les idéaux fermés de A.

b) Soit $A = \mathcal{H}(\mathbb{C})$ l'anneau des fonctions holomorphes dans tout le plan complexe :
– A est intègre de corps des fractions les fonctions méromorphes sur $\mathbb{C}$;
– A n'est pas noethérien.
– $A^\times$ est l'ensemble des fonctions holomorphes qui ne s'annulent pas sur $\mathbb{C}$; $f \in A$ est inversible si et seulement si $f = \exp(g)$ pour $g \in A$;
– les éléments irréductibles de A sont les fonctions possédant un unique zéro simple ; en particulier A n'est pas factoriel ;
– A est intégralement clos.

c) Soit D le disque unité ouvert de $\mathbb{C}$, $\bar{D}$ le disque unité fermé. On note $\mathcal{A}(D)$ l'ensemble des fonctions continues sur $\bar{D}$ et holomorphes sur D. L'algèbre $\mathcal{A}(D)$ munie de la norme de la convergence uniforme est alors de Banach :
– l'ensemble des polynômes complexes est dense dans $\mathcal{A}(D)$;
– Soient $f_1, \cdots, f_n$ $(n \geq 2)$ des éléments de $\mathcal{A}(D)$, n'ayant pas de zéros communs ; l'idéal I qu'ils engendrent est $\mathcal{A}(D)$ tout entier ;
– les idéaux maximaux de $\mathcal{A}(D)$ sont les $\{f \in \mathcal{A}(D),\ f(\alpha) = 0\}$ où $\alpha \in \bar{D}$.

d) anneaux de fonctions p-adiques (de Roba...)

III- *Modules*

a) sur un anneau principal : théorème de structure avec pour applications
– théorème de la base adaptée ;
– groupes abéliens de type fini
– invariants de similitude.

b) localisation (définition et premières propriétés) avec pour application
– anneaux des décimaux
– anneau local (complété) : exemples $\mathbb{Z}_{(p)}$ $(\mathbb{Z}_p)$ et $K[X]_{(X)}$ $(K[[X]])$
– lemme de Nakayama qui permet de ramener l'étude d'un module M sur un anneau local A à celle du $k = A/\mathcal{M}$ espace vectoriel $M/\mathcal{M}M$, où $\mathcal{M}$ désigne l'unique idéal maximal de A.

c) Les premiers associés à un module M sont les premiers P qui sont des annulateur d'un $m \in M$.

IV- *Equations diophantiennes*

La difficulté de leur résolution tient au fait que l'on mélange les structures multiplicatives et additives de $\mathbb{Z}$ dans une seule et même équation. On cherche alors tout naturellement à factoriser l'équation : en général celle-ci ne se factorise pas dans $\mathbb{Z}$ ce qui nous amène à

introduire une extension finie K de $\mathbb{Q}$ telle que l'équation se factorise dans la clôture intégrale $\mathcal{O}_K$ de $\mathbb{Z}$ dans K.

a) Dans le cas où $\mathcal{O}_K$ est principal, nous avons déjà mentionner les exemples suivants :
– cas $n = 2$ et 3 de l'équation de Fermat ;
– étude de l'ensemble des n qui sont de la forme $x^2 + py^2$ avec $p = 1$ ou 2 ou 3.

b) Groupe de classes d'idéaux : dans un anneau de Dedekind tout idéal s'écrit de manière unique comme un produit d'idéaux premiers. On considère alors le groupe des idéaux fractionnaires de $\mathcal{O}_K$ que l'on quotiente par les idéaux fractionnaires principaux : le groupe obtenu s'appelle le groupe des classes, il est de cardinal fini noté h_K. Kummer a alors remarqué que si dans l'équation de Fermat pour $n = p$ premier, le groupe de classes de $\mathbb{Q}[e^{2i\pi/p}]$ était premier avec p, on pouvait faire comme si l'anneau $\mathbb{Z}[e^{2i\pi/p}]$ était principal. Comme illustration on propose l'énoncé suivant :

Soit $d > 1$ sans facteurs carrés avec $d \equiv 1, 2 \mod 4$. Supposons que le nombre de classes de $\mathbb{Q}(i\sqrt{d})$ n'est pas divisible par 3. Alors $y^2 = x^3 - d$ a une solution entière si et seulement si d est de la forme $3t^2 \pm 1$ auquel ses solutions sont $(t^2 + d, \pm t(t^2 - 3d))$.

c) Soit $f(x, y) = ax^2 + bxy + cy^2$ une forme quadratique primitive définie positive de discriminant D. On lui associe l'idéal fractionnaire $I_f :=< 1, \tau_f >$, où $\tau_f = \frac{-b+i\sqrt{-D}}{2a} >$, de l'anneau des entiers $\mathcal{O}_K$ du corps quadratique imaginaire $K = \mathbb{Q}(i\sqrt{-D})$. Cette application $f \mapsto I_f$ induit alors une bijection de l'ensemble des classes d'équivalence sous $SL_2(\mathbb{Z})$ des formes quadratiques définies positives de discriminant D avec les classes d'idéaux fractionnaires de $\mathcal{O}_K$. La loi de groupe induite par $Cl(K)$ sur les formes quadratiques correspond alors à la notion de composition de formes quadratiques découverte par Gauss.

d) adèles et idèles avec comme application le traitement complet de la détermination des premiers p qui peuvent s'écrire sous la forme $x^2 + ny^2$ via un peu de théorie du corps de classes

V- *Calcul formel via les base de Gröbner*

a) idéaux monomiaux de $K[x_1, \cdots, x_n]$: ce sont ceux qui possède un ensemble fini de générateurs qui sont des monômes. Une des particularité bien pratique des idéaux monomiaux est la suivante : *Soit $\mathfrak{A}$ un idéal monomial de $K[x_1, \cdots, x_n]$ et $f = \sum_i c_i m_i$ avec $c_i \in K\{0\}$ et m_i des monômes distincts. Alors $f \in \mathfrak{A}$ si et seulement si pour tout i, $m_i \in \mathfrak{A}$.*

On en déduit alors le **lemme de Dickson** (cf. [**4**] 3.2.1) : *tout idéal monomial de $K[x_1, \cdots, x_n]$ est finiment engendré.*

b) généralisation de la division euclidienne : on suppose fixée une relation d'ordre totale sur les monômes de $K[x_1, \cdots, x_n]$ qui soit compatible à la multiplication. Pour $f = \sum_{i=1}^{N} c_i m_i$ avec $0 \neq c_i \in K$ et $m_1 > m_2 > \cdots > m_N$ des monômes, *le support* de f est $\{m_i : i = 1, \cdots, N\}$, son *monôme dominant* est $md(f) = m_1$, *son coefficient dominant* est $cd(f) = c_1$ et *son terme dominant* est $td(f) = c_1 m_1$. Pour $\mathfrak{A} =< f_1, \cdots, f_r >$, on note $d(\mathfrak{A}) =< md(f) : f \in \mathfrak{A} >$.

Définition : soient $f, g_1, \cdots, g_s \in K[x_1, \cdots, x_n]$, le reste de f modulo $g_1, \cdots, g_s$, noté $R(f, (g_1, \cdots, g_s))$ est défini comme suit :
– soit k minimal, s'il existe, tel que $md(g_k)$ divise $md(f)$, alors $R(f, (g_1, \cdots, g_s)) = R(f - ng_k, (g_1, \cdots, g_s))$ où n est tel que $td(f) = td(ng_k)$;
– si aucun des $md(g_k)$ divise $md(f)$ alors $R(f, (g_1, \cdots, g_s)) = td(f) + R(f - td(f), (g_1, \cdots, g_s))$.

Remarque : il est clair que ce processus est fini et définit uniquement $R(f,(g_1,\cdots,g_s))$ qui est une généralisation de la division euclidienne dans le cas $n=1$. En général $R(f,(g_1,\cdots,g_s))$ dépend de l'ordre des éléments $g_1,\cdots,g_s$.
Définition : un ensemble $\{g_1,\cdots,g_s\}$ d'éléments d'un idéal $\mathfrak{A}$ de $K[x_1,\cdots,x_n]$ est appelée une base de Gröbner si $d(\mathfrak{A}) =< md(g_1),\cdots,md(g_s) >$.
Remarque : On peut alors montrer que tout idéal $\mathfrak{A}$ admet une unique base de Gröbner réduite et on dispose d'algorithme pour la calculer.

c) Applications au calcul formel : le système d'équations polynomiales

$$\begin{cases} f_1(x_1,\cdots,x_n)=0 \\ \qquad\vdots \\ f_r(x_1,\cdots,x_n)=0 \end{cases}$$

- a des solutions si et seulement si 1 appartient à toute base de Gröbner.
- a un nombre fini de solutions si et seulement si, étant donnée une base de Gröbner $(g_1,\cdots,g_s)$ de $\mathfrak{A} =< f_1,\cdots,f_r >$:

$$\forall i=1,\cdots,n,\ \exists m_i\in\mathbb{N} \text{ tel que } x_i^{m_i}\in\{md(g_1),\cdots,md(g_s)\}.$$

Voici dans le même genre quelques questions réponses sur le thème :
- $g\in\mathbb{C}[x_1,\cdots,x_n]$ appartient-il à un idéal $\mathfrak{A}$? On construit une base de Gröbner $(f_1,\cdots,f_r)$ de $\mathfrak{A}$ et on calcule $R(g,(f_1,\cdots,f_r))$. Si ce dernier est nul alors $g\in\mathfrak{A}$ sinon $g\notin\mathfrak{A}$.
- Une autre question habituelle est de savoir si toute solution de $f_1=f_2=\cdots=f_r=0$ est aussi solution de $g=0$ ce qui, d'après le Nullstellensatz, revient à savoir si g appartient au radical $\sqrt{< f_1,\cdots,f_r >}$. La réponse est alors positive si et seulement si $< f_1,\cdots,f_r,1-yg >=\mathbb{C}[x_1,\cdots,x_n,y]$: en effet si $< f_1,\cdots,f_r,1-yg >$ est un idéal strict de $\mathbb{C}[x_1,\cdots,x_n,y]$, il existe alors $(x_1,\cdots,x_n,y)\in\mathbb{C}^{n+1}$ tel que $f_1(x_1,\cdots,x_n)=\cdots=f_r(x_1,\cdots,x_n)=1-yg(x_1,\cdots,x_n)=0$ et donc $1=0$. Réciproquement s'il existe des polynômes $a_1,\cdots,a_r,z\in\mathbb{C}[x_1,\cdots,x_n,y]$ tels que $1=a_1f_1+\cdots+a_rf_r+z(1-yg)$. En spécialisant en un point $(x_1,\cdots,x_n)$ tel que $f_1=\cdots=f_r=0$ et $g\neq 0$, on obtient dans $\mathbb{C}[y]$, $1=z(1-yg(x_1,\cdots,x_n))$ ce qui n'est pas car $1-yg(x_1,\cdots,x_n)$ est un polynôme de degré plus grand que 1.

  Ainsi il suffit de construire une base de Gröbner de $< f_1,\cdots,f_r,1-yg >$ et de tester si 1 en est un élément.
- Une des applications principales des bases de Gröbner en calcul formel, est leur aptitude à simplifier des expressions modulo des relations. Supposons que $x_1,\cdots,x_n$ soient des variables liées par des relations

$$(R)\quad f_1(x_1,\cdots,x_n)=0,\cdots,f_r(x_1,\cdots,x_n)=0$$

  alors simplifier une expression $g(x_1,\cdots,x_n)$ modulo les relations (R), c'est tout simplement calculer l'image de g dans le quotient $K[x_1,\cdots,x_n]/\mathfrak{A}$ avec $\mathfrak{A} =< f_1,\cdots,f_r >$. Connaissant une base de Gröbner, il suffit alors de calculer $R(g,(f_1,\cdots,f_r))$, c'est ce que fait la fonction Maple *simplify*.
- Étant donné un idéal $\mathfrak{A}$ de $K[x_1,\cdots,x_m,y_1,\cdots,y_n]$, le problème de *l'élimination* est de déterminer $\mathfrak{A}\cap K[y_1,\cdots,y_n]$. Or étant donnés une base de Gröbner de $\mathfrak{A}$ relativement à un ordre tel que tous les x_i sont plus grands que n'importe quel monôme en les y_j, $G\cap K[y_1,\cdots,y_n]$ est alors une base de Gröbner de $\mathfrak{A}\cap K[y_1,\cdots,y_n]$. En effet on a $G\cap K[y_1,\cdots,y_n]\subset\mathfrak{A}\cap K[y_1,\cdots,y_n]$ et si $f\in\mathfrak{A}\cap K[y_1,\cdots,y_n]$ alors $R(f,G)=0$. Or

d'après la définition de $R(f,G)$ les différents calculs ne font intervenir que des éléments de $G \cap K[y_1, \cdots, y_n]$ de sorte que $R(f, G \cap K[y_1, \cdots, y_n]) = 0$, d'où le résultat.

VI- *Géométrie algébrique*

La géométrie algébrique consiste en un pont entre l'algèbre (ici) commutative, i.e. l'étude des anneaux et de leurs modules, et la géométrie : l'idée générale est de considérer un anneau A comme l'anneau des fonctions sur un espace X : on retrouve X comme l'ensemble des idéaux maximaux ou premiers de A.

Exemples : :

- Les idéaux premiers de $k[X,Y]$ sont (0), (f) pour $f(X,Y)$ irréductible, et les idéaux maximaux $\mathcal{M} = (p,g)$ avec $p(X) \in k[X]$ irréductible non constant et $g \in k[X,Y]$ tel que sa réduction modulo p est un irréductible de $k[X]/(p)[Y]$. En particulier $k[X,Y]/\mathcal{M}$ est une extension algébrique finie de k.
- Les idéaux premiers de $\mathbb{Z}[Y]$ sont (0), (f) pour $f \in \mathbb{Z}[Y]$ irréductible, et les idéaux maximaux $\mathcal{M} = (p,g)$ avec $p \in Nm$ premier et $g \in \mathbb{Z}[Y]$ tel que sa réduction modulo p est irréductible dans $\mathbb{F}_p[Y]$. En particulier $\mathbb{Z}[Y]/\mathcal{M}$ est une extension finie de $\mathbb{F}_p$.

a) - définition du radical d'un idéal et lien avec le nilradical de A/I (un exemple sur $\mathbb{Z}$ est bienvenu).

- Pour S une partie de $K[X_1, \cdots, X_n]$, on note $\mathcal{V}(S) = \{x \in K^n : \forall P \in S \; P(x) = 0\}$. Pour $B \subset K^n$, on note $\mathcal{I}(B) = \{P \in K[X_1, \cdots, X_n] : \; P(b) = 0 \forall b \in B\}$. Ainsi par exemple une variété non vide V est irréductible (i.e. V n'est pas la réunion de deux sous-variétés propres) si et seulement si $\mathcal{I}(V)$ est un idéal premier.

b) Comme toute variété est une union de variétés irréductibles, on pourrait espérer que tout idéal d'un anneau noethérien est une intersection d'idéaux premiers ; cependant l'exemple de (X^2) dans $K[X]$ ôte tout espoir ; la bonne notion est celle de décomposition primaire et des idéaux premiers associés, cf. plus haut.

c) Nullstellensatz faible : si L est une K-algèbre de type fini alors $K \subset L$ est une extension finie ; en application citons

- les idéaux maximaux de $K[X_1, \cdots, X_n]$ sont de la forme $(X_1 - x_1, \cdots, X_n - x_n)$:
- soit le système $P_i(X_1, \cdots, X_n)$ pour $i = 1, \cdots, m$ admet une solution soit il existe $Q_1, \cdots, Q_m \in K[X_1, \cdots, X_n]$ tels que $P_1Q_1 + \cdots + Q_mP_m = 1$;
- si I est un idéal propre de $K[X_1, \cdots, X_n]$ alors $V(I) \neq \emptyset$;

d) Nullstellensatz fort : on a $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$;

e) Pour un anneau A, Spec$A$ désigne l'ensemble des idéaux premiers de A. *La topologie de Zariski* sur Spec$A$ est celle dont l'ensemble des fermés sont les

$$\mathbb{V}(I) = \{P \in \text{Spec}A : \; P \supset I\}$$

où I est un idéal de A. On définit aussi pour $X \subset \text{Spec}A$, $\mathbb{I}(X) = \bigcap_{P \in X} P$. En particulier on a $\overline{\mathcal{V}(I) - \mathcal{V}(J)} \subset \mathcal{V}(I : J)$.

e) Notion de dimension : la codimension d'un idéal premier P est la longueur maximale d'un chaine d'idéaux premiers contenus dans P. Pour un idéal I quelconque, sa codimension est la plus petite codimension des idéaux premiers le contenant.

Exemples la chaine $(x) \subset (x,y) \subset I = (x,y,z)$ est maximale (localisez et quotientez...) de sorte que I est de codimension 3 dans $k[x,y,z]$ ce qui correspond bien à la codimention de l'origine dans l'espace k^3.

La dimension de Krull d'un anneau A est la longueur maximale d'une chaine d'idéaux premiers de A. Un anneau de polynômes est *caténaire*, i.e. deux chaines d'idéaux premiers

entre deux idéaux premiers P et Q ont la même longueur de sorte qu'en particulier on a $codim(I) = dim(A) - dim(A/I)$.

1.1. Développements. —
- $\mathbb{Z}[i]$ est principal, application au théorème des deux carrés [**5**]
- les idéaux maximaux de $\mathbb{Z}[X]$ [**?**]
- les idéaux maximaux de $\mathbb{C}[X_1, \cdots, X_n]$ (Nullstellensatz) [**1**] ou de $k[X, Y]$ [**3**]
- A noethérien implique $A[X]$ noethérien [**5**]
- théorème de la base adaptée [**6**]
- tout idéal à engendrement fini de $\mathcal{H}(\mathbb{C})$ est principal [**?**]
- résolution de l'équation diophantienne $y^2 = x^3 - d$ pour $d \equiv 1, 2 \mod 4$;
- groupe de classes d'idéaux et composition des formes quadratiques à la Gauss [**2**]
- généralisation de la division euclidienne via les bases de Grobner [**4**]

2. Questions

Exercice 2.1. — *Soit A un anneau intègre.*

(a) Un idéal strict de A est dit maximal s'il l'est pour l'inclusion, i.e. le seul idéal qui le contienne est A lui-même. Montrez que $\mathcal{M}$ est un idéal maximal de A si et seulement si $A/\mathcal{M}$ est un corps. En utilisant le lemme de Zorn, montrez l'existence d'idéaux maximaux.

(b) Un idéal $\mathcal{P}$ de A est dit premier s'il vérifie la propriété suivante :

$$xy \in \mathcal{P} \text{ et } x \notin \mathcal{P} \Rightarrow y \in \mathcal{P}$$

Montrez que $\mathcal{P}$ est un idéal premier de A si et seulement si $A/\mathcal{P}$ est intègre.

(c) Soient $\mathcal{P}$ un idéal premier de A et $I_1, \cdots, I_r$ des idéaux tels que $I_1.\cdots.I_r \subset \mathcal{P}$. Montrez que $\mathcal{P}$ contient l'un des I_k.

(d) Soit I un idéal non premier de A, montrez qu'il existe deux idéaux I_1 et I_2 tels que $I \subset I_1$, $I \subset I_2$ et $I_1.I_2 \subset I$.
En utilisant le lemme de Zorn, montrez l'existence d'idéaux premiers minimaux pour l'inclusion. En supposant A noethérien, montrez qu'il existe un nombre fini d'idéaux premiers minimaux.

(e) Un idéal $\mathcal{Q}$ sera dit primaire s'il vérifie :

$$\forall x, y \in A \; xy \in \mathcal{Q}, \; x \notin \mathcal{Q} \Rightarrow \exists n \; y^n \in \mathcal{Q}.$$

Si $\mathcal{Q}$ est primaire que peut-on dire de $A/\mathcal{Q}$? Pour tout idéal I de A, on pose

$$\sqrt{I} = \{x \in A \; / \; \exists n \; x^n \in I\}.$$

Montrer que Q primaire entraine que sa racine est un idéal premier. Réciproquement : soit $I = (X)$, $n > 1$ $J = (X, Y)^n$ dans $A = \mathbb{C}[X, Y]$. Montrer que $Q = I \cap J$ n'est pas primaire bien que son radical soit premier.

Exercice 2.2. — *Soient $\mathfrak{A}$ et $\mathfrak{B}$ des idéaux d'un anneau A. On définit alors*

$$\mathfrak{A} : \mathfrak{B} = \{a \in A : \; ab \in \mathfrak{A} \; \forall b \in \mathfrak{B}\}$$

Montrez que $\mathfrak{A} : \mathfrak{B}$ est un idéal de A tel que :

(i) $(\mathfrak{A} : \mathfrak{C}) + (\mathfrak{B} : \mathfrak{C}) \subset (\mathfrak{A} + \mathfrak{B}) : \mathfrak{C}$ *;*

(ii) $\mathfrak{A} : (\mathfrak{B} + \mathfrak{C}) = (\mathfrak{A} : \mathfrak{B}) \cap (\mathfrak{A} : \mathfrak{C})$ *;*

(iii) $(\mathfrak{A} : \mathfrak{B}) : \mathfrak{C} = \mathfrak{A} : (\mathfrak{B}\mathfrak{C})$ *;*

Exercice 2.3. — *Quels sont les idéaux bilatères de* $\mathcal{L}(E)$ *?*

Exercice 2.4. — *Quels sont les idéaux à gauche de* $\mathcal{L}(E)$ *?*

Exercice 2.5. — *Quels sont les idéaux à droite de* $\mathcal{L}(E)$ *?*

Exercice 2.6. — *Soit* k *un corps et* $A = k[[X]]$ *l'algèbre des séries formelles à coefficients dans* k*.*

(i) Montrez que A *est intègre et déterminez* $A^\times$*.*

(ii) Montrez que tout idéal non nul de A *est de la forme* $X^n A$*,* $n \in \mathbb{N}$*. En déduire que* A *est principal et déterminez ses éléments irréductibles.*

(iii) Montrez que A *est euclidien.*

Exercice 2.7. — *On note* $A = \mathbb{Z}[i] = \{a + ib \ / \ (a, b) \in \mathbb{Z}^2\}$*, l'anneau des entiers de Gauss. Pour* $z = a + ib \in A$*, on pose* $N(a + ib) = a^2 + b^2$*.*

(i) Montrez que N *est multiplicative, i.e.* $N(zz') = N(z)N(z')$ *et en déduire que* $A^\times = \{\pm 1, \pm i\}$ *ainsi que l'identité de Lagrange :*

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$$

(ii) En remarquant que tout nombre complexe peut s'écrire comme la somme d'un élément de $\mathbb{Z}[i]$ *et d'un nombre complexe de module strictement plus petit que* 1*, en déduire que* A *est euclidien mais que la division euclidienne n'est pas unique.*

(iii) Soit $S = \{n \in \mathbb{N} \ / \ \exists (a, b) \in \mathbb{N}^2 n = a^2 + b^2\}$*. Montrer que* S *est une partie multiplicative de* $\mathbb{N}$*.*

(iv) Soit p *un nombre premier. Montrez l'équivalence des points suivants :*

- *p est irréductible dans A ;*
- *$p = 3 \mod (4)$*
- *$p \notin S$.*

(v) En déduire que les éléments irréductibles de A *modulo les unités, sont les* p *premiers congrus à* 3 *modulo* 4 *et les* $a + ib$ *tels que* $a^2 + b^2$ *est premier.*

(vi) Montrez que si $n \geq 2$*, alors* $n \in S$ *si et seulement si la multiplicité* $v_p(n)$ *de* p *dans* n *est paire pour tout* $p \equiv 3 \mod 4$ *(théorème des deux carrés).*

Exercice 2.8. — *Soit* $A := \mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5} \ / \ (a, b) \in \mathbb{Z}^2\}$*. On introduit comme d'habitude l'application* $N : a + ib\sqrt{5} \in A \mapsto a^2 + 5b^2 \in \mathbb{N}$*. On rappelle qu'un élément* $z \in A$ *est dit irréductible si et seulement si il vérifie la propriété suivante :*

$$z = z_1 z_2 \text{ et } z_1 \notin A^\times \Rightarrow z_2 \in A^\times$$

(i) Montrez que $z \in A^\times$ *si et seulement si* $N(z) = 1$ *puis que si* $N(z)$ *est un nombre premier alors* z *est irréductible.*

(ii) En étudiant l'égalité

$$3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5}),$$

montrez que $\mathbb{Z}[i\sqrt{5}]$ *n'est pas factoriel.*

(iii) Etudiez de même l'égalité $2.3 = a.b$ *avec* $a = 1 + i\sqrt{5}$ *et* $b = 1 - i\sqrt{5}$ *et montrez avec cet exemple que le lemme de Gauss n'est pas vérifié et que* $2a$*,* ab *n'ont pas de pgcd.*

Exercice 2.9. — *Trouver un exemple de deux entiers d'un corps quadratique qui ont même norme sans être ni conjugués ni associés.*

Exercice 2.10. — *Montrer que, si $\epsilon \in \mathbb{Q}(\sqrt{d})$ est une unité de norme 1 d'un corps quadratique, il existe un entier γ tel que $\epsilon = \frac{\gamma}{\gamma'}$, où γ' est le conjugué de γ.*

Exercice 2.11. — *Montrer qu'un entier algébrique dont tous les conjugués (dans $\mathbb{C}$) sont de module strictement inférieur à 1 est forcément nul.*

Exercice 2.12. — *Montrer que, dans un corps de nombres K de degré n, tout idéal (entier) non nul contient une infinité d'entiers naturels mais que, si b est un entier naturel non nul, il n'est pas contenu dans plus de b^n idéaux entiers.*

Exercice 2.13. — *Dans $K = \mathbb{Q}(\theta = \sqrt[4]{5})$, calculer les discriminants*

$$\Delta(1, \theta, \theta^2, \theta^3),$$

$$\Delta(1+\theta, 1+\theta^2, 1+\theta^3, 1+\theta^4)$$

$$\Delta(1, \theta, \frac{1+\theta^2}{2}, \frac{\theta+\theta^3}{2}).$$

Exercice 2.14. — *Donnez une base de l'anneau $\mathcal{O}_K$ des entiers de $K = \mathbb{Q}(\sqrt{2}, i)$.*

Exercice 2.15. — ***Corps cyclotomiques*** *Soit p premier et $K = \mathbb{Q}(\xi)$ où $\xi = e^{\frac{2i\pi}{p}}$ et on note $\mathcal{O}_K$ son anneau des entiers.*

(1) Calculez la trace d'un élément de K.
(2) Montrez que la norme de $1-\xi$ est égale à p.
(3) Soit $\alpha = a_0 + a_1\xi + \cdots + a_{p-2}\xi^{p-2} \in \mathcal{O}_K$.
  (i) En considérant $\alpha\xi^{-k} - \alpha\xi$, montrez que $b_k = pa_k \in \mathbb{Z}$.
  (ii) On pose $\lambda = 1-\xi$, montrez que $p\alpha = c_0 + c_1\lambda + \cdots + c_{p-2}\lambda^{p-2}$ avec $c_i \in p\mathbb{Z}$.
  (iii) Conclure que $a_k \in \mathbb{Z}$ et donc que $\mathcal{O}_K = \mathbb{Z}[\xi]$.
  (iv) Montrez que le discriminant de K est $(-1)^{(p-1)/2}p^{p-2}$.
(4) Traitez le cas de $\mathbb{Q}(e^{2i\pi/n})$ avec n quelconque.

Exercice 2.16. — *Montrez que l'anneau des entiers de $\mathbb{Q}(i\sqrt{d})$ est euclidien pour $d = 1, 2, 3, 7, 11$.*

Exercice 2.17. — *Pour $d > 11$ sans facteurs carré, montrez que $\mathbb{Q}(i\sqrt{d})$ n'est pas euclidien.*

Exercice 2.18. — *On considère le corps $K = \mathbb{Q}(\sqrt{-43})$. On pose $\omega = \frac{-1+\sqrt{-43}}{2}$, et on rappelle que l'anneau des entiers de K admet $\{1, \omega\}$ comme base sur $\mathbb{Z}$.*

(1) Calculer le polynôme minimal de ω sur $\mathbb{Q}$. Montrer que 2 et 3 sont inertes dans K.
(2) Calculer la constante de Minkowski de K. Montrer que $\mathcal{O}$ est principal.
(3) Soit $\alpha \notin \mathbb{Z}$ un élément de $\mathcal{O}$ qui engendre un idéal premier. Montrer que $N_{L/\mathbb{Q}}(\alpha)$ est un nombre premier.
(4) Soit x et $y \neq 0$ deux entiers premiers entre eux tels que $x^2 + xy + 11y^2$ soit strictement inférieur à 121. Montrer que $x^2 + xy + 11y^2$ est un nombre premier.

3. Solutions

2.1 (a) Soit $\mathcal{M}$ un idéal maximal de A et soit $\bar{a} \in A/\mathcal{M}$ non nul. On fixe $a \in A$ d'image $\bar{a}$ par la projection naturelle $\pi : A \to A/\mathcal{M}$; ainsi $a \notin \mathcal{M}$ de sorte que l'idéal engendré par a et $\mathcal{M}$ est strictement plus grand que $\mathcal{M}$ et donc par maximalité est égal à A. On en déduit donc l'existence d'éléments $\lambda \in A$ et $m \in MC$ tels que $1 = \lambda a + m$, soit $\bar{1} = \bar{\lambda}\bar{a}$ et donc $\bar{a}$ est inversible d'inverse $\bar{l}$.
Réciproquement soit I un idéal contenant $\mathcal{M}$ strictement et soit $x \in I\backslash\mathcal{M}$, de sorte que $\bar{x}$ est non nul dans $A/\mathcal{M}$ et donc inversible : $\bar{1} = \bar{x}\bar{y}$ soit $1 - xy \in \mathcal{M}$ pour $y \in \bar{y}$, et donc $1 \in I$ soit $I = A$.

Pour utiliser le lemme de Zorn, il suffit de montrer que la relation d'ordre sur l'ensemble $\mathcal{I}$ des idéaux, définie par l'inclusion est inductive, i.e. que toute chaîne totalement ordonnée C admet un majorant, à savoir $M = \cup_{I\in C} I$. Vérifions que M est bien un idéal soient $x, y \in M$, et $I \subset J \in C$ tel que $x \in I$, $y \in J$; on a alors $x, y \in J$ et donc $x - y \in J \subset M$. On démontre de même que si $x \in M$ et $a \in A$ alors $ax \in M$. Le lemme de Zorn affirme alors l'existence d'éléments maximaux, qui sont donc des idéaux maximaux.

(b) La traduction est immédiate : la relation $\bar{x}\bar{y} = \bar{0}$ est équivalente à $xy \in \mathcal{P}$ pour $x \in \bar{x}$ et $y \in \bar{y}$; ainsi si $\mathcal{P}$ est premier on a x ou y appartient à $\mathcal{P}$ soit $\bar{x} = \bar{0}$ ou $\bar{y} = \bar{0}$. Réciproquement si $xy \in \mathcal{P}$ alors si $A/\mathcal{P}$ est intègre, on a $\bar{x} = \bar{0}$ ou $\bar{y} = \bar{0}$ et donc x ou y appartient à $\mathcal{P}$.

(c) Soit $\mathcal{P}$ premier et $I_1 \cdots I_r \subset \mathcal{P}$, et supposons que pour tout $1 \leq k \leq r$, $I_k \not\subset \mathcal{P}$; on fixe ainsi pour tout k, un élément $x_k \in I_k$ et $x_k \notin \mathcal{P}$. Par hypothèse $x_1 \cdots x_r \in \mathcal{P}$ avec $x_1 \notin \mathcal{P}$ soit $x_2 \cdots x_r \in \mathcal{P}$ et par récurrence $x_r \in \mathcal{P}$ d'où la contradiction.

(d) Soit I non premier, et soit $x, y \in A\backslash I$ avec $xy \in I$. On pose $I_1 = (I \cup \{x\})$ et $I_2 = (I \cup \{y\})$; on a $I_1 I_2 \subset I$ avec $I \subset I_1 \cap I_2$.

On considère la relation d'ordre sur l'ensemble $\mathcal{I}$ des idéaux premiers, donnée par la contenance, i.e. $I \leq J \Leftrightarrow J \subset I$; cette relation d'ordre est à nouveau inductive, un majorant d'une chaîne totalement ordonnée C étant donné par l'intersection $M = \cap_{I\in C} I$; en effet on vérifie comme précédemment que M est un idéal, le fait qu'il soit premier se montre aisément : soit $xy \in M$ et donc $xy \in I$ pour tout $I \in C$; comme I est premier, x ou y appartient à I ; supposons que $y \notin I$, alors pour tout $J \subset I \in C$, on a $y \notin J$ et donc $x \in J$ soit $x \in M$. Le lemme de Zorn donne alors l'existence d'éléments maximaux qui sont donc des idéaux premiers minimaux pour l'inclusion.

On suppose A noethérien et on considère l'idéal (0) ; s'il est premier alors c'est le seul idéal premier minimal, sinon soit I_1 et I_2 comme ci-dessus. Si I_1 et I_2 sont premiers, ceux sont les seuls idéaux premiers minimaux ; en effet soit $\mathcal{P}$ un idéal premier ; on a $(0) = I_1 I_2 \subset \mathcal{P}$ et donc $I_i \subset \mathcal{P}$ pour $i = 1$ ou 2, d'après ce qui précède. Si I_1 n'est pas premier, soit $I_{1,1}$ et $I_{1,2}$ comme ci-dessus ; on construit ainsi un arbre binaire dont la racine est l'idéal (0), tous les sommets sont des idéaux qui contiennent le produit des idéaux de ses deux fils et tel que tout chemin filial défini une chaîne totalement ordonnée pour l'inclusion. Si on suppose A noethérien, l'arbre est fini et les idéaux premiers minimaux sont les feuilles.

(e) La traduction dans $A/\mathbb{Q}$ est à nouveau immédiate : $\mathbb{Q}$ est primaire si et seulement si dans $A/\mathbb{Q}$ les seuls diviseurs de 0 sont les éléments nilpotents, i.e. ceux tels qu'il existe n tels qu'élevés à la puissance n, ils donnent 0.
Montrons en premier lieu que $\sqrt{I}$ est un idéal : soient donc $x, y \in \sqrt{I}$ et n, m des entiers tels que $x^n \in I$ et $y^m \in I$. On a alors $(x+y)^{n+m-1} = \sum_{k=0}^{n+m-1} C^k_{n+m-1} x^k (-y)^{n+m-1-k}$; or $k < n$ si et seulement si $n + m - 1 - k \geq m$ et donc pour tout $0 \leq k \leq n + m - 1$, au moins un

parmi x^k et $y^{n+m-1-k}$ appartient à I et donc $x-y \in \sqrt{I}$. Si $a \in A$ alors $(ax)^n \in I$ et donc $ax \in \sqrt{I}$ et donc finalement $\sqrt{I}$ est un idéal de A.
Exemple : dans $\mathbb{Z}$, la racine de l'idéal $n\mathbb{Z}$ avec $n = \prod_i p_i^{\alpha_i}$ est l'idéal engendré par $\prod_i p_i$.

Soit $\mathbb{Q}$ un idéal primaire et $\mathcal{P} = \sqrt{\mathbb{Q}}$; soit $x, y \in A$ tels que $xy \in \mathcal{P}$ et $x \notin \mathcal{P}$. Soit donc un entier n tel que $x^n y^n \in \mathbb{Q}$; comme $x \notin \mathcal{P}$ alors $x^n \notin \mathbb{Q}$ et donc $\mathbb{Q}$ étant primaire, soit m un entier tel que $(y^n)^m \in \mathbb{Q}$ soit $y \in \mathcal{P}$, et donc $\mathcal{P}$ est un idéal premier.

On considère $A = \mathbb{C}[X, Y]$ l'anneau des polynômes en deux variables à coefficients dans $\mathbb{C}$ et soit $I = (X)$ et $J = (X, Y)^n$ avec $n > 1$. On pose $\mathbb{Q} = I \cap J$ qui est l'idéal engendré par $X^n, X^{n-1}Y, \cdots, XY^{n-1}$; on a $\sqrt{\mathbb{Q}} = (X)$ qui est premier alors que $\mathbb{Q}$ n'est pas primaire car $X^{n-1}Y \in \mathbb{Q}$ avec $X^{n-1} \notin \mathbb{Q}$ et $Y^m \notin \mathbb{Q}$ pour tout entier m.

2.2 Vérifions tout d'abord que $\mathfrak{A} : \mathfrak{B}$ est un idéal de A : soient $a_1, a_2 \in \mathfrak{A} : \mathfrak{B}$ et $a \in A$, pour tout $b \in \mathfrak{B}$ on a $(r_1 + ar_2)b = r_1 + ar_2 b \in \mathfrak{A}$, d'où le résultat.

(i) Soit $a = a_1 + a_2 \in \mathfrak{A} : \mathfrak{C} + \mathfrak{B} : \mathfrak{C}$ de sorte que pour tout $c \in \mathfrak{C}$, $a_1 c \in \mathfrak{A}$ et $a_2 c \in \mathfrak{B}$ et donc $ac \in \mathfrak{A} + \mathfrak{B}$ pour tout $c \in \mathfrak{C}$ soit $a \in (\mathfrak{A} + \mathfrak{B}) : \mathfrak{C}$.

(ii) Soit $a \in \mathfrak{A} : (\mathfrak{B} + \mathfrak{C})$ alors $a(b + c) \in \mathfrak{A}$ pour tout $b \in \mathfrak{B}$ et $c \in \mathfrak{C}$. En particulier en prenant $c = 0$, on a $ab \in \mathfrak{A}$ pour tout $b \in \mathfrak{B}$ et donc $a \in \mathfrak{A} : \mathfrak{B}$. En procédant de même avec $\mathfrak{C}$, on obtient l'inclusion $\mathfrak{A} : (\mathfrak{B} + \mathfrak{C}) \subset (\mathfrak{A} : \mathfrak{B}) \cap (\mathfrak{A} : \mathfrak{C})$. Réciproquement soit $a \in (\mathfrak{A} : \mathfrak{B}) \cap (\mathfrak{A} : \mathfrak{C})$ alors $ab \in \mathfrak{A}$ pour tout $b \in \mathfrak{G}$ et $ac \in \mathfrak{A}$ pour tout $c \in \mathfrak{C}$ de sorte que $a(b + c) \in \mathfrak{A}$, ce qui donne l'inclusion réciproque.

(iii) Soit $a \in (\mathfrak{A} : \mathfrak{B}) : \mathfrak{C}$ de sorte que pour tout $c \in \mathfrak{C}$, $ac \in \mathfrak{A} : \mathfrak{B}$ et donc pour tout $b \in \mathfrak{B}$, on a $acb \in \mathfrak{A}$. Comme $\mathfrak{A}$ est stable par l'addition, on en déduit donc que $ad \in \mathfrak{A}$ pour tout $d \in \mathfrak{B}\mathfrak{C}$ et donc $(\mathfrak{A} : \mathfrak{B}) : \mathfrak{C} \subset \mathfrak{A} : (\mathfrak{B}\mathfrak{C})$. Réciproquement soit $a \in \mathfrak{A} : (\mathfrak{B}\mathfrak{C})$ de sorte que pour tout $d \in \mathfrak{B}\mathfrak{C}$, on a $ad \in \mathfrak{A}$. En particulier pour $d = bc$, c fixé et b décrivant $\mathfrak{C}$, on obtient que $ac \in \mathfrak{A} : \mathfrak{B}$. Comme ce fait est vrai pour tout c, on en déduit que $a \in (AF : \mathfrak{B}) : \mathfrak{C}$.

2.3 On se ramène à $\mathbb{M}_n(K)$; soit I un idéal bilatère de $\mathbb{M}_n(K)$ et $M = (m_{i,j})_{1 \leq i,j \leq n} \in I$ non nulle. Soit (i_0, j_0) tel que $m_{i_0,j_0} \neq 0$. On a

$$E_{i,i_0} M E_{j_0,j} = \sum_{1 \leq k,l \leq n} m_{k,l} E_{i,i_0} E_{k,l} E_{j_0,j} = \sum_{k=1}^{n} m_{k,j_0} E_{i,i_0} E_{k,l} = m_{i_0,j_0} E_{i,j}$$

de sorte que pour tout (i, j), $E_{i,j} \in I$ et donc $I = \mathbb{M}_n(K)$.

2.4 Soit I un idéal de $\mathbb{M}_n(\mathbb{C})$, on va montrer que $I = \mathbb{M}_n(\mathbb{C})A = \{M \in \mathbb{M}_n(\mathbb{C}) \ / \ \operatorname{Ker} A \subset \operatorname{Ker} M\}$. Soit $M = PI_rQ \in I$, on a alors $Q^{-1}P^{-1}M \in I$ et donc I contient un projecteur. Pour tout f, on note I_f l'ensemble des endomorphismes qui s'annulent sur $\operatorname{Ker} f$: $I_f = \mathbb{M}_n(\mathbb{C})f$. De l'écriture $I = p + (Id - p)$, on en déduit que $\mathbb{M}_n(\mathbb{C}) = I_p \oplus I_{Id-p}$.

Soit alors p un projecteur de rang maximal dans I, alors $I \cap I_{Id-p} = 0$. En effet il suffit de montrer que l'intersection ne contient aucun projecteur q. Soit donc un projecteur q qui s'annule sur $\operatorname{Ker}(Id - p) = \operatorname{Im} p$. Dans une base convenable on a $p = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$ er $q = \begin{pmatrix} 0 & B \\ 0 & D \end{pmatrix}$. Le projecteur $r = \begin{pmatrix} 0 & 0 \\ 0 & D \end{pmatrix}$ appartient évidemment à I ainsi donc que $p + r$ de sorte que $D = 0$ et donc $\operatorname{tr} q = 0$ soit $q = 0$.

Ainsi on a $I = I_p$ d'où le résultat.

2.5 La réponse est $\{M \in \mathbb{M}_n(\mathbb{C}) \ / \ \operatorname{Im} M \subset \operatorname{Im} A\}$, la démonstration est parallèle à la précédente.

2.6 : (i) Soit ν la valuation sur $k[[X]]$ définie par $\nu(\sum_{i=0}^{+\infty} a_i X^i) = \min\{i \in \mathbb{N},\ a_i \neq 0\}$ avec la convention $\nu(0) = +\infty$. Ainsi si $a = \sum_i a_i X^i$ et $b = \sum_i b_i X^i$ sont de valuations respectives α, β, alors ab est de valuation $\alpha + \beta$ car $a_\alpha b_\beta \neq 0$.
Montrons que $a = \sum_i a_i X^i$ est inversible si et seulement si $a_0 \neq 0$; supposons $a_0 \neq 0$, la recherche d'un inverse se ramène à la résolution du système triangulaire suivant : $a_0 b_0 = 1$ et pour tout $k \geq 1$, $\sum_{i=0}^{k} a_i b_{k-i} = 0$; une solution se calculant facilement par récurrence sur k. Réciproquement si a a pour inverse $b = \sum_i b_i X^i$, on a alors $a_0 b_0 = 1$ et donc $a_0 \neq 0$.

(ii) Soit I un idéal non nul de A et soient $n = \min_{x \in I} \nu(x)$ et $a \in I$ tel que $\nu(a) = n$; $a = X^n b$ avec $\nu(b) = 0$ de sorte que b est inversible soit $X^n \in I$ et donc $(X^n) \subset I$; l'inclusion réciproque étant évidente, on en déduit $I = (X^n)$.
L'anneau A est donc principal, donc factoriel. Soit $p \in A$ un élément irréductible, l'idéal (p) est alors premier et maximal. Or tout idéal I est contenu dans (X) qui est maximal car si $b \notin (X)$ alors b est inversible ; ainsi on a $(a) = (X)$ et a est associé à X de sorte qu'aux inversibles près, il n'y a qu'un seul irréductible, à savoir X.

(iii) Montrons que A est euclidien pour le stathme ν. Soient donc $(a, b) \in A \times A^\times$; $b = X^n \beta$ avec $\beta \in A^\times$. On écrit $a\beta^{-1} = X^\beta q + c$ avec $\deg c < \beta$, et donc $a = c\beta + bq$ avec $c\beta = 0$ ou $\nu(c\beta) < \nu(b) = \beta$, d'où le résultat.

2.7 : (a) La démonstration est classique ; soit I un idéal de A et soit $b \neq 0 \in I$ tel que $v(b)$ est minimal. Pour $i \in I$, on effectue une division euclidienne de i par b : $i = bq + r$ avec $v(r) < v(b)$ et $r \in I$; d'après la minimalité de $v(b)$, on en déduit $r = 0$ et donc $I = (b)$.

(b) (i) L'application N est clairement multiplicative ; si $z \in A^\times$, on a $zz' = 1$ et donc $N(z)N(z') = 1$ soit $N(z) = 1$ et finalement $z = \pm 1, \pm i$. L'égalité $N((a + ib)(c + id)) = N(a + ib)N(c + id)$ donne l'identité remarquable de Lagrange.

(ii) Soit z_1 et z_2 des éléments de A ; on écrit $z_1/z_2 = q + e$ avec $q \in A$ et $e \in \mathbb{C}$ de module strictement plus petit que 1. On a alors $z_1 = qz_2 + r$ avec $r = z_2 e = z_1 - qz_2 \in A$ et $N(r) < N(z_2)$. Le choix de q n'est pas unique en général comme on peut le voir sur le dessin.

(iii) Le fait que S est une partie multiplicative découle directement de l'identité de Lagrange.

(iv) On rappelle que p est irréductible si et seulement si $A/(p)$ est intègre ; or $A/(p) \simeq \mathbb{Z}/p\mathbb{Z}[X]/(X^2+1)$ qui est intègre si et seulement si X^2+1 n'a pas de racines dans $\mathbb{Z}/p\mathbb{Z}$, soit si et seulement si (-1) n'est pas un carré modulo p et donc si et seulement si $p \equiv 3 \mod 4$. En outre $n \in S$ si et seulement si il existe $z \in A$ tel que $n = N(z)$ de sorte que si $p \in S$, on a $p = z\bar{z}$ avec $N(z) = p$ et donc $z, \bar{z}$ non inversible, soit p non irréductible. Réciproquement si p n'est pas irréductible, on a $p = zz'$ avec $z' = \bar{z}$ et donc $p = N(z) \in S$.

(v) Soit p premier congru à 3 modulo 4 alors p est irréductible dans A. De même si $N(z)$ est premier, z est irréductible car $z = xy$ implique $N(x)N(y)$ premier soit $N(x)$ ou $N(y)$ est égal à 1, i.e. x ou y est inversible.
Montrons qu'aux inversibles près, ce sont les seuls ; soit z irréductible et p premier divisant $N(z)$. Si $p \equiv 3 \mod 4$, alors p est irréductible et $p|z\bar{z}$ et donc $p|z$ et $p|\bar{z}$, soit z est associé à p. Si $p = 2$ ou $p \equiv 1 \mod 4$, on a $p = a^2 + b^2$ soit $a + ib$ irréductible et divise p donc z, soit z associé à $a + ib$, cqfd.

(vi) Soit $n \geq 2$ et supposons que pour tout $p \equiv 3 \mod 4$, $v_p(n)$ est pair. Pour montrer que $n \in S$, il suffit de montrer que pour tout p, $p^{v_p(n)} \in S$. Le résultat est clair pour $p \equiv 3 \mod 4$ car $v_p(n)$ est pair ; pour $p = 2$ et $p \equiv 1 \mod 4$, on a $p \in S$ et donc $p^{v_p(n)} \in S$.
Réciproquement, montrons par récurrence sur $n \geq 2$, l'implication réciproque : le cas $n = 2$ est trivial et pour $n \geq 3$, $n = a^2 + b^2$, si $p \equiv 3 \mod 4$ premier, divise n, alors p divise $(a+ib)(a-ib)$; or p est irréductible dans A de sorte que p divise $a+ib$ et $a-ib$, soit p divise

a et b ; ainsi $n = p^2((a/p)^2 + (b/p)^2)$ et $n/p^2 \in S$. Par hypothèse de récurrence $v_p(n/p^2)$ est pair et donc $v_p(n)$ aussi.

2.8 (i) L'application N est bien sur multiplicative, i.e. $N(zz') = N(z)N(z')$, à valeur dans $\mathbb{N}$. Si z est inversible, on en déduit qu'il existe z' tel que $zz' = 1$ soit $N(z)N(z') = 1$ ce qui impose $N(z) = 1$. Réciproquement si on a $N(z) = z\bar{z} = 1$ alors $\bar{z}$ est l'inverse de z.

Soit alors z tel que $N(z)$ est premier ; soit $z_1 z_2 = z$ avec z_1 non inversible, il s'agit alors de montrer que z_2 l'est. On a donc $N(z) = N(z_1)N(z_2)$ et donc $N(z_2) = 1$ et $z_2 \in A^\times$.

(ii) On va montrer que si z est tel que $N(z) = 9$ alors z est irréductible de sorte que 3, $2 \pm i\sqrt{5}$ sont tous irréductibles, et l'égalité $3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$ sont deux factorisation distinctes en produit d'irréductibles. Soit donc $z \in \mathbb{Z}[i\sqrt{5}]$ tel que $N(z) = 9$; on écrit $z = z_1 z_2$ avec $N(z_1) \neq 1$. On a donc $N(z) = 9 = N(z_1)N(z_2)$; or les factorisations de 9 dans $\mathbb{N}$, sont 3×3 et 9×1. On remarque que $N(a + ib\sqrt{5}) = a^2 + 5b^2 = 3$ est impossible, de sorte $N(z_2) = 1$ soit z_2 inversible..

(ii) De la même façon, si $N(z) = 4, 6$, alors z est irréductible de sorte que $2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ est un autre contre-exemple à l'unicité de la décomposition en produit d'irréductibles. En particulier 2 irréductible divise $6 = ab$ et 2 ne divise ni a, ni b. Soit δ un éventuel pgcd de $2a$ et ab ; on a 2 et a qui divise δ, de sorte que $N(\delta)$ est un multiple de 4 et de 6 et donc un multiple de 12. De la même façon comme d divise 6 et $2a$, on en déduit que $N(\delta)$ divise 36 et 24 et donc leur pgcd qui est 12. Ainsi on obtiendrait $N(\delta) = 12 = a^2 + 5b^2$ qui n'a pas de solutions, d'où la contradiction.

2.9 Dans l'anneau $\mathbb{Z}[i]$ des entiers de Gauß, qui est l'anneau des entiers de $\mathbb{Q}[i]$ et qui est principal, un nombre premier p est décomposé si et seulement si il est congru à 1 modulo 4. Dans ce cas, il se décompose en produit de deux entiers conjugués entre eux et premiers entre eux. par exemple $5 = (1+2i)(1-2i)$. Pour répondre à la question, on pourrait se contenter de prendre $\alpha = 1+2i$ et $\beta = i(1-2i) = 2-i$, mais ce serait tricher : β est associé au conjugué de α. Mais si nous prenons un autre nombre premier décomposé, par exemple $13 = (2+3i)(2-3i)$, il suffit de prendre $\alpha = (1+2i)(2+3i) = -4+7i$ et $\beta = (1+2i)(2-3i) = 8+i$ pour avoir un exemple : $65 = 5.13 = 4^2 + 7^2 = 8^2 + 1$ s'écrit comme somme de deux carrés de deux façons essentiellement différentes, contrairement à 5 et à 13.

2.10 Soit α un entier quelconque de K. On pose $\gamma = \alpha + \alpha'\epsilon$. On a $\epsilon\gamma' = \epsilon(\alpha' + \alpha\epsilon') = \gamma$. Pour conclure, il reste à prouver que l'on peut choisir α de façon à ce que γ ne soit pas nul. Si $\epsilon \neq -1$, on peut prendre $\alpha = 1$, sinon on prend $\alpha = \sqrt{d}$.

2.11 Soit α un tel entier, de degré n, $\kappa < 1$ le plus grand module d'un conjugué de α et k un entier tel que $\kappa^k < 2^{-n}$. Considérons l'entier algébrique $\beta = \alpha^k$. Les coefficients de son polynôme caractéristique sont sommes de produits de conjugués de β : chaque conjugué est de module inférieur à κ^k et chaque somme comporte moins de 2^n termes. Ces coefficients sont donc des entiers rationnels de valeur absolue strictement inférieure à 1, c'est-à-dire qu'ils sont nuls. Le polynôme caractéristique de β est X^n et $\alpha = \beta = 0$.

2.12 Tout idéal entier non nul $\mathfrak{a}$ contient sa norme, qui est un entier naturel non nul. Il contient aussi tous les multiples de cette norme, qui sont en nombre infini. Inversement, comme indiqué dans l'introduction, tout idéal qui contient b est engendré par b et un autre entier, disons x. Exprimons x dans une base d'entiers, et réduisons ses composantes modulo b. Le nombre de valeurs possibles de x est inférieur ou égal à b^n, d'où le résultat. Il est facile de voir que, même pour $n = 1$, cette majoration est grossière.

2.13 Comme indiqué dans le cours, le discriminant de la base $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ où θ est racine d'un polynôme F irréductible de degré n vaut $(-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(F'(\theta))$. Ici $F = X^4 - 5$, donc $F'(\theta) = 4\theta^3$ et

$$\Delta(1, \theta, \theta^2, \theta^3) = N_{K/\mathbb{Q}}(F'(\theta)) = 4^4 N_{K/Q}(\theta)^3 = 4^4.(-5)^3 = -32000.$$

Compte tenu de l'égalité $\theta^4 = 5$, la matrice de passage de la première base à la deuxième est

$$\begin{pmatrix} 1 & 0 & 0 & 6 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

et son déterminant est -6. On en déduit

$$\Delta(1 + \theta, 1 + \theta^2, 1 + \theta^3, 1 + \theta^4) = 6^2.\Delta(1, \theta, \theta^2, \theta^3) = -1152000.$$

De même, la matrice

$$\begin{pmatrix} 1 & 0 & 1/2 & 0 \\ 0 & 1 & 0 & 1/2 \\ 0 & 0 & 1/2 & 0 \\ 0 & 0 & 0 & 1/2 \end{pmatrix}$$

a pour déterminant $1/4$, ce qui donne

$$\Delta(1, \theta, \frac{1 + \theta^2}{2}, \frac{\theta + \theta^3}{2}) = 4^{-2}.\Delta(1, \theta, \theta^2, \theta^3) = -2000.$$

2.14 On considère le $\mathbb{Z}$-module R engendré par $1, \sqrt{2}, i, i\sqrt{2}$ dont le discriminant est 64. On a aussi

$$N(a + b\sqrt{2} + ci + di\sqrt{2}) = (a^2 - c^2 - 2b^2 + 2d^2)^2 + 4(ac - 2bd)^2$$

On commence par regarder si $r/2$ peut être entier, i.e. si 16 peut diviser $(a^2 - c^2 - 2b^2 + 2d^2)^2 + 4(ac - 2bd)^2$ pour $a, b, c, d = 0, 1$ sans qu'ils soient tous nuls. On trouve alors $b = d = 1$ et $a = c = 0$ soit donc $\alpha = \frac{\sqrt{2}+i\sqrt{2}}{2}$ avec $\alpha^2 = i$ et donc $\alpha^4 + 1 = 0$ qui est bien entier.

On considère alors R' engendré par $1, \sqrt{2}, i, i\sqrt{2}, \frac{\sqrt{2}(1+i)}{2})$ qui est donc engendré par $1, \sqrt{2}, i, \frac{\sqrt{2}(1+i)}{2}$ avec $\Delta_{R'} = -16$. Il faut alors vérifier qu'aucun $r'/2$ nouveau n'est entier...

2.15 (1) La trace de ξ^i est $T(\xi^i) = T(\xi) = \xi + \xi^2 + \cdots + \xi^{p-1} = -1$ de sorte que

$$T(\sum_{i=0}^{p-2} a_i \xi^i) = (p-1)a_0 - \sum_{i=1}^{p-2} a_i = pa_0 - \sum_{i=0}^{p-2} a_i$$

(2) La norme de $1 - \xi$ est $N(1 - \xi) = \prod_{i=1}^{p-1}(1 - \xi^i) = \Phi_p(\xi) = p$.

(3) (i) On a $T(\alpha\xi^{-k} - \alpha\xi) = T(a_0\xi^{-k} + \cdots + a_k + \cdots + a_{p-2}\xi^{p-k-2} - a_0\xi - \cdots - a_{p-2}\xi^{p-1})$ qui est donc égal à $pa_k - (a_0 + \cdots + a_{p-2}) - (-a_0 - \cdots - a_{p-2}) = pa_k$.

(ii) On substituant $1 - \lambda$ à ξ dans $p\alpha = b_0 + \cdots + b_{p-2}\xi^{p-2}$ on obtient

$$c_i = \sum_{j=i}^{p-2} (-1)^i \binom{i}{j} b_j \in \mathbb{Z} \qquad b_i = \sum_{j=i}^{p-2} (-1)^i \binom{i}{j} c_j$$

En particulier on a $c_0 = b_0 + \cdots + b_{p-2} = p(-T(\alpha) + b_0)$ et donc $p|c_0$. Supposons alors que pour $k \geq 0$, et pour tous $i \leq k-1$, les c_i sont divisibles par p. De l'égalité

$$p = N(1-\xi) = (1-\xi)^{p-1} \prod_{i=1}^{p-1} (1 + \xi + \cdots + \xi^{i-1}) = \lambda^{p-1}\kappa$$

on en déduit que p appartient à l'idéal (λ^{p-1}) de $\mathcal{O}_K$ car $\kappa \in \mathbb{Z}[\xi] \subset \mathcal{O}_K$. On reprend alors l'égalité $p\alpha = c_0 + \cdots + c_{p-2}\lambda^{p-2}$ que l'on regarde modulo (λ^{k+1}) ce qui donne $c_k\lambda^k \equiv 0 \mod (\lambda^{k+1})$ et donc $c_k = \mu\lambda$ pour $\mu \in \mathcal{O}_K$. En prenant les normes on obtient $c_k^{p-1} = pN(\mu)$ et donc p divise c_k.

(iii) On en déduit alors que p divise b_k et donc $a_k \in \mathbb{Z}$ ce qui prouve que $\mathcal{O}_K \subset \mathbb{Z}[\xi]$ et donc l'égalité.

(iv) Le discriminant de K est donc égal à $(-1)^{(p-1)(p-2)/2} N(\Phi_p'(\xi))$ avec $\Phi_p(X) = \frac{X^p-1}{X-1}$ et donc $\Phi_p'(\xi) = \frac{-p\xi^{p-1}}{\lambda}$ de sorte que $N(\Phi_p'(\xi)) = p^{p-2}$.

2.16 Le sthasme est la norme et la preuve est identique à celle de $\mathbb{Z}[i]$ en notant que pour $d = 3, 7, 11$, l'anneau des entiers est $\mathbb{Z}[\frac{1+i\sqrt{d}}{2}]$.

2.17 On raisonne par l'absurde en considérant un sthasme ψ (qui à priori n'est pas la norme !). Soit alors $\alpha \in \mathcal{O}_K$ qui n'est pas une unité et tel que $\psi(\alpha)$ soit minimal. Pour tout $\beta \in \mathcal{O}_K$, il existe alors $q, r \in \mathcal{O}_K$ tels que $\beta = q\alpha + r$ avec $\psi(r) < \psi(\alpha)$ de sorte que $r = 0$ ou r est une unité. Or pour $d > 11$ les seules unités sont ± 1 de sorte que $\mathcal{O}_K/(\alpha)$ est de cardinal inférieur ou égal à 3. Or d'après le cours ce cardinal est égal à la norme de α. Si $-d \equiv 1 \mod 4$, on a $\alpha = a + i\sqrt{d}b$ avec $a^2 + db^2 \leq 3$ soit $a = \pm 1$ et $b = 0$ de sorte que α serait une unité ce qui n'est pas. Si $-d \not\equiv 1 \mod 4$, on a $\alpha = \frac{a+i\sqrt{d}b}{2}$ avec donc $a^2 + db^2 \leq 12$ ce qui redonne α inversible, d'où la contradiction.

Remarque : Pour $\mathbb{Q}(\sqrt{d})$, la question est beaucoup plus difficile et il a fallu attendre 1950 pour y répondre définitivement.

2.18 (1) On a $Tr(\omega) = \omega + \omega' = -1$ et $N(\omega) = \omega\omega' = 11$. Le polynôme minimal de ω est donc $X^2 + X + 11$. Modulo 2 ou 3, ce polynôme est irréductible. La première proposition permet de conclure : 2 et 3 sont encore premiers dans K.

(2) Ici, $n = 2$, $t = 1$ et $D_K = 43$. La formule donne donc

$$M_K = \frac{4}{\pi}\frac{2}{4}\sqrt{43} = \frac{2\sqrt{43}}{\pi} < 5.$$

On vient de voir qu'il n'y a pas d'idéal de norme 2 ou 3, et que le seul idéal entier de norme 4 est $2\mathcal{O}$, qui est principal. Le théorème de Minkowski permet donc de conclure que K est principal.

(3) La norme d'un idéal premier d'un corps quadratique est soit un nombre premier ramifié ou décomposé, soit le carré p^2 d'un nombre premier inerte p. Mais dans ce dernier cas, l'idéal en question est forcément $p\mathcal{O}$. Si $\alpha\mathcal{O}$ et $p\mathcal{O}$ sont égaux, α/p est une unité de $\mathcal{O}$. Or, les seules unités de $\mathcal{O}$ sont 1 et -1. Cela contredirait l'hypothèse selon laquelle α n'appartient pas à $\mathbb{Z}$.

(4) La norme d'un entier de K qui n'est pas dans $\mathbb{Z}$ vaut $\frac{u^2+43v^2}{4} \geq \frac{43}{4}$, et comme c'est un entier, elle vaut au moins 11. Considérons l'entier $\alpha = x + y\omega$. Il n'appartient pas à $\mathbb{Z}$ puisque $y \neq 0$. Sa norme vaut $\alpha\alpha' = x^2 + xy + 11y^2 < 121$. Si ce n'était pas un nombre premier, il y aurait un diviseur premier de α de norme inférieure à 11, et, d'après ce qui précède, son générateur a serait dans $\mathbb{Z}$. Mais si un entier rationnel a divise α, il divise x et y, une contradiction.

On en déduit en particulier que $x^2 + x + 11$ est un nombre premier pour x compris entre 0 et 9. Le même raisonnement avec $\mathbb{Q}(\sqrt{-163})$ montre que $x^2 + x + 41$ est premier pour x allant de 0 à 39.

Références

[1] A. Chenciner. *Courbes algébriques planes*. Paris 7, 1979.

[2] D. Cox. *Primes of the form $x^2 + ny^2$*. Pure and applied mathematics. 1989.

[3] S. Francinou and Gianella H. *Exercices de mathématiques pour l'agrégation algèbre 1*. Masson, 1994.

[4] R. Fröberg. *An introduction to Gröbner Bases*. Pure and applied mathematics, 1998.

[5] D. Perrin. *Cours d'algèbre*. Ellipses, 1998.

[6] P. Samuel. *Théorie algébrique des nombres*. Hermann, 1967.