Dans ce cours tous les anneaux sont supposés commutatifs.

1. Notions d'algèbre commutative

1.1. **Idéaux d'un anneau.** Considérons deux équations algébriques, par exemple l'équation d'un cercle, $F(X,Y) = X^2 + Y^2 - 1$, ainsi que l'équation d'une droite, $G(X,Y) = X + Y - 1$. L'ensemble Z des solutions communes de ces deux équations est l'ensemble des points (x,y) de $\mathbf{C}^2$ tels que $F(x,y) = G(x,y) = 0$. Il est clair que l'ensemble Z est le lieu des solutions de bien d'autres systèmes d'équations algébriques et il n'est pas toujours facile de choisir un système d'équations plutôt qu'un autre pour étudier Z. C'est pourquoi il est souvent commode de considérer l'ensemble des équations dont Z est solution. Cet ensemble est une partie de l'ensemble $\mathbf{C}[X,Y]$ des polynômes en deux variables et possède une structure particulière, la structure d'idéal que nous allons étudier dans cette partie.

Définition 1.1. *Soit A un anneau. Un idéal de A est une partie I de A telle que $(I,+)$ est un sous-groupe de $(A,+)$ et qui est de plus stable par multiplication par tout élément de A, autrement dit, pour tous $a \in A$ et $x \in I$, on a $ax \in I$.*

Remarquons tout de suite que comme $(I,+)$ est un sous-groupe de $(A,+)$, I contient l'élément neutre pour l'addition, c'est-à-dire 0. En particulier I est une partie non vide de A et contient toujours 0.

Exemple 1.2. 1. L'ensemble $\{0\}$ est un idéal appelé idéal nul.

2. L'ensemble A tout entier est lui aussi un idéal de A.
3. Si I et J sont des idéaux de A, l'ensemble $I \cap J$ est un idéal de A.
4. Si I et J sont des idéaux de A, on définit $I + J$ par
$$I + J = \{x + y,\ x \in I,\ y \in J\},$$
il s'agit d'un idéal de A.
5. Si I et J sont des idéaux de A, on veut définir l'idéal produit de I et J, c'est-à-dire une partie de A qui est un idéal et qui contient tous les produits d'éléments de I par des éléments de J. Il est naturel de définir
$$IJ = \{\sum_i x_i y_i,\ x_i \in I,\ y_i \in J\}.$$
L'ensemble IJ est alors un idéal de A et $IJ \subset I \cap J$. Il faut prendre garde au fait que cette inclusion n'est en général pas une égalité.
6. Si $x \in A$, on note Ax l'ensemble $\{ax,\ a \in A\}$ des multiples de x. Il s'agit d'un idéal de A. Les idéaux de cette forme sont dits monogènes.

En règle générale, si I est un idéal de A, l'élément 1 n'appartient pas à I. En effet, si $1 \in I$, alors pour tout $a \in A$, on a $a = a1 \in I$ et donc $I = A$. Ainsi $1 \in I$ si et seulement si $I = A$.

Définition 1.3. *Un idéal I de A est dit de type fini, s'il existe des éléments $x_1, \ldots, x_n$ de A tels que $I = Ax_1 + \cdots + Ax_n$.*

Une notation couramment utilisée pour désigner l'idéal $Ax_1 + \cdots + Ax_n$ est également $(x_1, \ldots, x_n)$.

1.2. **Anneaux quotients.** Soient A et B deux anneaux et soit f un morphisme d'anneaux de A vers B. Le noyau $\ker f$ de f est toujours un idéal de A. Réciproquement, la construction qui va suivre montre que tout idéal de I est le noyau d'un morphisme surjectif entre anneaux.

Soit I un idéal de A. On définit une relation d'équivalence sur A en posant $x \sim_I y$ si et seulement si $x - y \in I$. On note A/I l'ensemble des classes d'équivalence pour la relation $\sim_I$. Si $x \in A$, on note $[x]$ la classe de x, autrement dit l'ensemble $x + I$. On peut munir l'ensemble A/I d'une structure d'anneau en posant $[x]+[y] = [x+y]$ et $[x][y] = [xy]$. Il est important de vérifier que cette définition est cohérente, c'est-à-dire que les classes $[x + y]$ et $[xy]$ sont indépendantes des choix faits pour les représentants x et y des classes $[x]$ et $[y]$.

Proposition 1.4. *L'application $q_I : x \mapsto [x]$ est un morphisme surjectif d'anneaux de A vers A/I dont le noyau est égal à l'idéal I.*

Remarque 1.5. La construction de la relation d'équivalence $\sim_I$ est une généralisation de la notion de congruence. En effet, si on considère l'anneau $A = \mathbf{Z}$ et l'idéal $I = \mathbf{Z}n$ alors la relation d'équivalence $\sim_I$ est exactement la relation de congruence modulo n et l'anneau quotient A/I est l'anneau $\mathbf{Z}/n\mathbf{Z}$.

Exemple 1.6. Soit k un corps et soit A l'anneau $k[X, Y]$ des polynômes en deux variables à coefficients dans k. On considère I l'idéal des multiples de Y. L'anneau A/I est alors isomorphe à l'anneau $k[X]$ des polynômes en une variable. Il suffit en effet de considérer le morphisme envoyant un polynôme $P(X, Y)$ sur le polynôme $P(X, 0)$ en une variable. En termes imagés, on a « ajouté la relation $Y = 0$ à l'anneau A ».

Rappelons qu'un anneau A est dit intègre s'il est non nul (c'est-à-dire $1 \neq 0$) et si pour tout $a \in A \smallsetminus \{0\}$ et $b \in A \smallsetminus \{0\}$, on a $ab \in A \smallsetminus \{0\}$.

Définition 1.7. *Un idéal I d'un anneau A est dit premier si l'anneau A/I est intègre. Il est dit maximal si l'anneau A/I est un corps.*

Un corps est cas particulier d'anneau intègre, en particulier un idéal maximal est un idéal premier. Si I est un idéal maximal d'un anneau A, si J est un autre idéal de A tel que $I \subset J \subset A$, alors soit $J = I$ soit $J = A$ (voir les exercices). Ceci justifie la terminologie « idéal maximal ».

Exemple 1.8. 1. Si $n \geqslant 0$, on sait que l'anneau $\mathbf{Z}/n\mathbf{Z}$ est un corps si et seulement si il est intègre si et seulement si n premier. Par conséquent l'idéal $\mathbf{Z}n$ de $\mathbf{Z}$ est maximal si et seulement si il est premier si et seulement si n est un nombre premier. Les idéaux premiers peuvent donc être perçus dans un premier temps comme des généralisations de la notion de nombre premier.

2. Soit k un corps. Considérons l'anneau $A = k[X,Y]$ et l'idéal $I = k[X,Y]Y$ engendré par Y. Comme l'anneau quotient A/I est isomorphe à l'anneau intègre $k[X]$, l'idéal I est premier. Cependant cet idéal n'est pas maximal. On peut le voir de deux façons. On peut soit remarquer que $k[X]$ n'est pas corps car, par exemple, l'élément X n'est pas inversible dans $k[X]$. On peut aussi remarquer qu'il existe une suite d'inclusions strictes d'idéaux $(Y) \subsetneq (X,Y) \subsetneq k[X,Y]$.
3. Si $(a_1, \ldots, a_n) \in k^n$, l'idéal $(X_1 - a_1, \cdots, X_n - a_n)$ de $k[X_1, \ldots, X_n]$ est maximal.

Nous admettons le résultat suivant qui est une conséquence du Lemme de Zorn.

Théorème 1.9 (Krull)**.** *Soit I un idéal de A différent de A. Alors il existe un idéal maximal de A contenant I.*

1.3. **Quelques classes d'anneaux.**

Définition 1.10. *Un anneau A est dit principal s'il est intègre et si tous ses idéaux sont principaux.*

Exemple 1.11. (1) Les anneaux $\mathbf{Z}$ et $k[X]$, pour k un corps, sont principaux.
(2) Si $n \geqslant 2$, l'anneau $k[X_1, \ldots, X_n]$ n'est pas principal.

Définition 1.12. *Soit A un anneau et soit $x \in A$. L'élément x est dit irréductible si x n'est pas inversible dans A et si $x = ab$ implique $a \in A^\times$ ou $b \in A^\times$.*

Exemple 1.13. Dans l'anneau $k[X,Y]$, les polynômes X et Y sont irréductibles.

Définition 1.14. *Un anneau A est dit factoriel s'il est intègre et si tout élément non nul de A s'écrit comme un produit d'éléments irréductibles avec unicité de cette écriture à permutation près et multiplication par des inversibles. Plus précisément si*

$$a = p_1 \cdots p_n = q_1 \cdots q_m$$

avec $p_1, \ldots, p_n, q_1, \ldots, q_m$ irréductibles, on a $n = m$ et il existe une bijection de $\{1, \ldots, n\}$ sur $\{1, \ldots, m\}$ ainsi que des éléments inversibles $a_1, \ldots, a_n$ tels que, pour tout $1 \leqslant i \leqslant n$, on a $p_i = a_i q_{\sigma(i)}$.

Les anneaux factoriels ont les propriétés suivantes.

Proposition 1.15. *Soit A un anneau factoriel et soit $x \in A$. Alors l'idéal principal (x) est premier si et seulement si x est irréductible.*

La propriété suivante est plus difficile à démontrer mais est bien pratique.

Proposition 1.16. *Soit A un anneau factoriel et soit K son corps des fractions. Un polynôme $P \in A[X]$ est irréductible si et seulement si il est irréductible dans $K[X]$ et ses coefficients sont premiers entre eux dans leur ensemble dans A.*

Exemple 1.17. (1) Un anneau principal est factoriel.

(2) Si A est factoriel, l'anneau $A[X]$ est factoriel.

(3) L'anneau $\mathbf{Z}[\mathrm{i}\sqrt{5}]$ est intègre mais n'est pas factoriel.

1.4. **L'anneau des polynômes multivariés.** Nous admettons le théorème suivant.

Théorème 1.18 (Hilbert)**.** *Soit k un corps. Tout idéal de $k[X_1, \dots, X_n]$ est de type fini.*

Nous pouvons à présent énoncer la version algébrique du théorème des zéros de Hilbert.

Rappelons que si k est un corps, un idéal maximal de $k[X]$ est de la forme (P) pour P un polynôme irréductible de $k[X]$. Le quotient $k[X]/(P)$ est alors un corps et une extension finie de k, appelé corps de rupture du polynôme P. Comme le montre le théorème ci-dessous, cette propriété se généralise aux k-algèbres de type fini.

Théorème 1.19. *Soit k un corps. Si $\mathfrak{m}$ est un idéal maximal de $k[X_1, \dots, X_n]$. Alors $k[X_1, \dots, X_n]/\mathfrak{m}$ est un corps et une extension finie de k.*

Remarque 1.20. Lorsque $n = 1$, c'est une conséquence immédiate du fait que l'anneau $k[X]$ est principal. Tout idéal de $k[X]$ est de la forme (P), c'est-à-dire engendré par un élément. Dès que $n \geqslant 2$, il existe dans $k[X_1, \dots, X_n]$ des idéaux non principaux.

Lorsque k est un corps algébriquement clos, on a une description complète des idéaux maximaux de $k[X_1, \dots, X_n]$.

Corollaire 1.21. *Soit k un corps algébriquement clos. L'application $(a_1, \dots, a_n) \mapsto (X_1 - a_1, \dots, X_n - a_n)$ est une bijection de k^n sur l'ensemble des idéaux maximaux de $k[X_1, \dots, X_n]$.*

Démonstration. Considérons $\mathfrak{m}$ un idéal maximal de $k[X_1, \dots, X_n]$ et posons $K := k[X_1, \dots, X_n]/\mathfrak{m}$. D'après le théorème 1.19, le corps K est une extension finie de k. Comme k est algébriquement clos, on a en fait $K = k$. Posons alors, pour $1 \leqslant i \leqslant n$, $a_i := q_{\mathfrak{m}}(X_i) \in k$. On a $q_{\mathfrak{m}}(X_i - a_i) = 0$ donc $(X_1 - a_1, \dots, X_n - a_n) \subset \mathfrak{m}$. Par maximalité de $\mathfrak{m}$, on en déduit l'égalité $(X_1 - a_1, \dots, X_n - a_n) = \mathfrak{m}$. □

Nous allons à présent donner une preuve du théorème 1.19 dans le cas où k est un corps infini non dénombrable (le corps $\mathbf{C}$ par exemple).

Preuve du théorème 1.21. Soit $\mathfrak{m}$ un idéal maximal de $k[X_1, \ldots, X_n]$. Posons $K := k[X_1, \ldots, X_n]/\mathfrak{m}$. Supposons par l'absurde que le corps K n'est pas une extension finie de k. Notons x_i l'image de X_i dans K. On a $K = k[x_1, \ldots, x_n]$. Si tous les x_i sont algébriques sur k, alors K est de dimension finie sur k. On peut donc supposer qu'il existe $1 \leqslant i \leqslant n$ tel que x_i est transcendant sur k. Ceci implique en particulier que K contient un sous-corps isomorphe au corps des fractions rationnelles $k(X)$. Le théorème de décomposition en éléments simples implique alors que la famille $\left(\frac{1}{X-a}\right)_{a \in k}$ est libre sur k. Comme k n'est pas pas dénombrable, cette famille ne l'est pas non plus. Ainsi le k-espace vectoriel K contient une famille libre non dénombrable. Par ailleurs la famille $(x_i^{k_i})_{(k_i) \in \mathbb{N}^n}$ est une famille génératrice de K qui de plus est dénombrable. Le k-espace vectoriel K contient une famille génératrice dénombrable et une famille libre indénombrable, c'est une contradiction. □

Définition 1.22. *Soit A un anneau, on appelle A-algèbre de type fini un anneau isomorphe à un quotient $A[X_1, \ldots, X_n]/I$ où I est un idéal de $A[X_1, \ldots, X_n]$.*

De façon équivalente, un anneau A est une k-algèbre de type fini si et seulement si il existe un morphisme surjectif d'anneaux $k[X_1, \ldots, X_n] \to A$.

Proposition 1.23. *Si A est une k-algèbre de type fini, tout idéal de A est de type fini.*

Démonstration. Soit I un idéal de A. Comme A est une k-algèbre de type fini, il existe un morphisme d'anneaux surjectif $f : k[X_1, \ldots, X_n] \twoheadrightarrow A$. L'ensemble $f^{-1}(I)$ est un idéal de $k[X_1, \ldots, X_n]$. D'après le théorème 1.18, c'est un idéal de type fini, disons engendré par des éléments $x_1, \ldots, x_r$. Comme $I = f(f^{-1}(I))$, on vérifie facilement que I est engendré par $f(x_1), \ldots, f(x_r)$ et donc est de type fini. □