Anneaux– Piqûre de rappel.

On présente ici le prérequis de théorie des anneaux pour le M1 d'algèbre.

1 Anneaux. idéaux.

Un anneau $(A, +, .)$ est un groupe abélien $(A, +)$ dont l'élément neutre sera noté 0_A ou 0, muni d'une opération interne notée "." vérifiant
A1. Associativité : $(a.b).c = a.(b.c)$
A2. Distributivité à gauche et à droite : $a.(b+c) = a.b+a.c$, $(b+c).a = b.a+c.a$.

Dans la suite on supposera que les anneaux sont commutatifs et unitaires, c'est à dire :
A3. $a.b = b.a$
A4. Il existe un élément unité 1 dans A tel que $1.a = a.1 = a$ pour tout a.

On se passera donc des anneaux de matrices, ou du corps des quaternions. Un (homo)morphisme d'anneaux f de A vers A' est une application qui vérifie :
H1. $f(a + b) = f(a) + f(b)$.
H2. $f(a.b) = f(a).f(b)$.
H3. $f(1_A) = 1_{A'}$.

Un sous-anneau B de A est un sous-groupe de $(A, +)$ qui est stable pour la multiplication.
Un idéal I de A est un sous-groupe de $(A, +)$ qui de plus vérifie :
I1. Si $a \in A$ et $b \in I$, alors $a.b \in I$.

Lorsque I est un idéal de A, alors il existe une structure d'anneau quotient sur A/I telle que :
Q1. $\overline{a} + \overline{b} = \overline{a + b}$.
Q2. $\overline{a}.\overline{b} = \overline{a.b}$.

On a le théorème fondamental de passage au quotient

Théorème 1 *Soit f un morphisme d'anneaux de A vers A' et $I = \ker f := \{a \in A,\ f(a) = 0_{A'}\}$. Alors,*
1. I est un idéal de A.
2. Si $J \subset I$ est un idéal de A, alors
2a. Il existe un morphisme d'anneaux $\overline{f}$ de A/J vers A' tel que $f = \overline{f}\pi$, où π désigne la projection canonique $\pi : A \to A/J$.
2b. $\ker \overline{f} = I/J$.
2c. $Im\overline{f} = Imf$.
3. On a en particulier, pour $J = I$, un isomorphisme entre A/I et Imf.
4. L'image réciproque d'un idéal de A par f est un idéal de A. (attention, l'image d'un idéal n'est en général pas un idéal.)

On peut faire des opérations sur les idéaux :
Définition. Soient I et J deux idéaux de A, alors on pose :
$I + J := \{x + y,\ x \in I,\ y \in J\}$.
$I.J := \{\sum_k x_k.y_k,\ x_k \in I,\ y_k \in J\}$, où la somme est finie.

On voit facilement que $I + J$ et $I.J$ sont encore des idéaux et on généralise cette définition à la somme et au produit d'un nombre fini d'idéaux. On voit également que $IJ \subset I \cap J$ qui est aussi un idéal.
Un idéal est dit principal s'il est engendré par un seul élément :
$I = (x) := \{ax,\ a \in A\}$.
Plus généralement, on dira qu'un idéal est de type fini s'il est engendré par une famille (finie) $x_1, x_2, \ldots, x_k : I = (x_1, x_2, \ldots, x_k) = \{a_1x_1 + a_2x_2 + \ldots + a_kx_k,\ a_i \in A\}$.

Exemple. Si A est l'anneau $\mathbb{Z}$ des entiers, tout idéal est principal et on a

$$(a) + (b) = (d),\ (a) \cap (b) = (m),\ (a).(b) = (ab),$$

où d et m sont respectivement le pgcd et le ppcm de a et b.

Certains anneaux ont des propriétés particulières, citons pour l'instant :
Définition. Un anneau est dit principal si tout idéal est principal. Un anneau A est dit intègre si

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

Un anneau est un corps (commutatif) si tout élément non nul de A est inversible, ce qui revient à dire que $(A\backslash 0, .)$ est un groupe abélien ou que ses seuls idéaux sont triviaux à faire en exercice ou voir dans [Perrin, II, Lemme 1.9]). Bien entendu tout corps est intègre.

Proposition 1 *Un idéal I de A est dit premier s'il vérifie une des conditions équivalentes suivantes :*
(i) $ab \in I \Rightarrow a \in I$ ou $b \in I$.
(ii) L'anneau A/I est intègre.

La proposition résulte directement du fait qu'un élément est dans I si et seulement si sa classe est nulle dans A/I.
Exemple. Dans $\mathbb{Z}$, (0) est un idéal premier ainsi que l'idéal (p) où p est un nombre premier.

Il faut savoir montrer en exercice la proposition suivante :

Proposition 2 *On a :*
(i) Tout sous-anneau d'un anneau intègre est encore intègre.
(ii) L'image réciproque d'un idéal premier par un morphisme d'anneaux est encore un idéal premier.

Preuve : (i) est clair de par la définition d'un anneau intègre.
Soit maintenant f un morphisme entre les anneaux A et B, et soit J un idéal premier de B et $I := f^{-1}(J)$. On considère le morphisme $g = \pi \circ f : A \to B/J$ où π est la surjection canonique $B \to B/J$. On a $\ker(g) = f^{-1}(\pi^{-1}(0)) = f^{-1}(J) = I$. Il en résulte un passage au quotient injectif $\overline{g} : A/I \hookrightarrow B/J$. Or, J est premier, donc B/J est intègre, et par (i), il vient que A/I l'est aussi, donc I est un idéal premier comme demandé. $\diamond$

Définition 1 *On appelle éléments inversibles ou unités de l'anneau A l'ensemble noté A^* des éléments de a tels qu'il existe b dans A tel que $a.b = 1$.*

Il est clair que $(A^*, .)$ est un groupe abélien. Si A est un corps, alors $A^* = A\backslash\{0\}$, si $A = \mathbb{Z}$, alors $A^* = \{\pm 1\}$, si $A = \mathbb{Z}/n\mathbb{Z}$, alors A^* est constitué des classes d'éléments premiers avec n.

Définition 2 *On dit que a divise b dans l'anneau A s'il existe c dans A tel que $b = ac$, c'est à dire si $(b) \subset (a)$. On dit que a et b sont associés si a divise b et b divise a, c'est à dire si et seulement si (a) et (b) définissent le même idéal .*

Proposition 3 *Supposons A intègre. Alors a et b sont associés si et seulement si il existe un élément c inversible tel que $a = b.c$.*

Preuve : Si $a = 0$, alors $b = 0$ et la proposition est claire dans ce cas. Supposons $a \neq 0$. Par hypothèse, $a = b.c$ et $b = a.d$, donc par substitution, $a = adc$. Comme a est non nul et A intègre, il vient que $dc = 1$ donc c est inversible. $\diamond$

2 Anneaux de polynômes.

Soit A un anneau. On construit l'anneau de polynômes $A[X]$ à indeterminée X comme étant l'ensemble

$$A[X] := \{\sum_{k\geq 0} a_k X^k,\ a_k \in A\},$$

où tous les a_k sont nuls sauf pour un nombre fini. On le munit d'une addition et d'une multiplication

$$(\sum_k a_k X^k) + (\sum_k b_k X^k) = \sum_k (a_k + b_k) X^k,\ (\sum_k a_k X^k).(\sum_k b_k X^k) = \sum_k c_k X^k,$$

où $c_k := \sum_{n+m=k} a_n b_m$.
On montre qu'il s'agit bien d'un anneau et l'application $\iota : A \to A[X]$, $a \mapsto aX^0$ est un morphisme injectif d'anneaux. On confondra donc A et son image dans $A[X]$. L'unité de $A[X]$ est alors confondue avec l'unité de A.

On définit ainsi par récurrence l'anneau à plusieurs indeterminées $A[X_1, \ldots, X_n] = A[X_1][\ldots][X_n]$. Il n'est pas inutile de le définir directement par analogie avec l'anneau à une seule indéterminée :
On note $X^\alpha = X_1^{\alpha_1} X_2^{\alpha_2} \ldots X_n^{\alpha_n}$, où $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{N}^n$. Alors

$$A[X_1, \ldots, X_n] := \{ \sum_{\alpha \in \mathbb{N}^n} a_\alpha X^\alpha,\ a_\alpha \in A \},$$

où tous les a_α sont nuls sauf pour un nombre fini. On le munit d'une addition et d'une multiplication

$$(\sum_\alpha a_\alpha X^\alpha) + (\sum_\alpha b_\alpha X^\alpha) = \sum_\alpha (a_\alpha + b_\alpha) X^\alpha,\ (\sum_\alpha a_\alpha X^\alpha).(\sum_\alpha b_\alpha X^\alpha) = \sum_\alpha c_\alpha X^\alpha,$$

où $c_\alpha := \sum_{\beta+\gamma=\alpha} a_\beta b_\gamma$.
La propriété fondamentale de l'anneau de polynômes à n indeterminées est similaire à la celle du groupe libre à n générateurs, mais dans le cadre des anneaux commutatifs.

Théorème 2 *Soit B un anneau commutatif. Alors la donnée d'un morphisme f de $A[X_1, X_2, \ldots, X_n]$ vers B est équivalente à la donnée de sa restriction à A et des images des X_i, c'est à dire de n éléments quelconques de B.*

Preuve : Bien entendu, si f existe alors on obtient de façon unique sa restriction g à A ainsi que les images des X_i.
Inversement, on se donne n morphismes g de A dans B ainsi que n éléments b_i, $1 \leq i \leq n$ de B. Alors, on définit $f : A[X_1, X_2, \ldots, X_n] \to B$ par

$$f(\sum_\alpha a_\alpha \prod_i X_i^{\alpha_i}) = \sum_\alpha g(a_\alpha) \prod_i b_i^{\alpha_i}.$$

L'application f est alors bien définie et c'est un morphisme d'anneau. Comme A et les X_i engendrent l'anneau $A[X_1, X_2, \ldots, X_n]$, il vient qu'une telle application vérifiant $f\ |_A = g$ et $f(X_i) = b_i$ est unique. $\diamond$
Ces morphismes sont souvent appelés morphismes d'évaluation en $X_i = b_i$.
Savoir faire : Montrer que $A[X,Y]/(X) \simeq A[Y]$. *On exhibe le morphisme d'évaluation en $X = 0$, ev : $A[X,Y] \to A[Y]$, $\sum_\alpha a_\alpha X^{\alpha_1} Y^{\alpha_2} \mapsto \sum_{\alpha_2} a_{(0,\alpha_2)} Y^{\alpha_2}$. Il est clair qu'il est surjectif et que son noyau est constitué des polynômes de $A[X,Y]$ factorisables par X, d'où l'isomorphisme par passage au quotient $A[X,Y]/(X) \simeq A[Y]$.*

Si A est un anneau intègre, alors $A[X]$ est aussi intègre et le degré du produit est égal la somme des degrés. Il vient alors que si A est intègre, alors les unités de $A[X]$ sont aussi les unités de A. C'est faux si A n'est pas intègre. Par exemple, si $A = \mathbb{Z}/4\mathbb{Z}$, alors $(1+2X)^2 = 1$ et donc $(1+2X)$ est inversible et de degré 1.