Chapitre 11

Anneaux et corps

11.1 Anneaux

11.1.1 La structure d'anneau

Définition 11.1 *Un anneau est triplet $(A, +, \times)$ tel que*
- *$(A, +)$ est un groupe commutatif,*
- *$\times$ est une loi interne sur A, associative.*
- *$\times$ est distributive par rapport à $+$, à droite et à gauche.*
- *Il existe un élément neutre pour la multiplication, souvent noté $\mathbf{1}_A$.*

Si $\times$ est commutative on parle d'anneau commutatif.

Remarque 11.1 *Antérieurement les anneaux ne possédaient pas nécessairement d'élement neutre pour la multiplication. On parlait d'anneau unitaire lorsqu'il existe un élément neutre pour la multiplication. La très grand majorité des anneaux étudiés dans le monde étant unitaires, on a intégré l'existence d'un élément neutre à la définition d'un anneau.*

Définition 11.2 *Un sous-anneau de $(A, +, \times)$, c'est un triplet $(B, +, \times)$ tel que*
- *B est unepartie de A telle que $(B, +)$ soit un sous-groupe de $(A, +)$,*
- *B est stable pour la loi $\times$,*
- *l'élément neutre*

.

Proposition 11.1 *Soit $(A_1, \ldots, A_p)$ une famille finie d'anneaux, dont les lois sont toutes représentée par $+$ pour l'addition et la concaténation pour la multiplication. Alors les lois*

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n),$$
$$(x_1, \ldots, x_n)(y_1, \ldots, y_n) = (x_1 y_1, \ldots, x_n y_n).$$

définissent deux lois sur $A_1 \times \cdots \times A_p$ qui en font un anneau, commutatif si tous les A_i le sont.

Remarque 11.2 *L'élément neutre, pour la multiplcation, de l'anneau $A_1 \times \cdots \times A_p$ est bien sûr $(\mathbf{1}_{A_1}, \cdots, \mathbf{1}_{A_p})$.*

Remarque 11.3 *Bien que cela ne soit pas évoqué par le programme une autre structure naturelle d'anneau est particulièrement naturelle, c'est l'ensemble $\mathcal{F}(X, A)$ des applications d'un ensemble X vers un anneau A, les lois étant définies par $f + g : x \mapsto f(x) + g(x)$ et $fg : x \mapsto f(x)g(x)$.*

Définition 11.3 *Un anneau A est intègre si et seulement si*

$$\forall (x,y) \in A^2 \qquad xy = 0 \Rightarrow x = 0 \text{ ou } y = 0.$$

Proposition 11.2 *Dans un anneau intègre tout élément non nul est régulier pour la multiplication.*

Définition 11.4 *Un anneau* **commutatif** *dans lequel tout élément non nul est inversible pour la multiplication s'appelle un corps.*

Remarque 11.4 *Dans le cadre strict du programme un corps est donc nécessairement commutatif. Auparavant un corps pouvait ne pas être commutatif. un théoème célèbre, le théorème de Wederburn s'énonçait tout corps fini est commutatif. Actuellement un anneau (unitaire) dans lequel tout élément non nul est inversible s'appelle une algèbre à division.*

La notion de sous-corps d'un corps se définit naturellement.

11.1.2 Morphismes

On note de manière conventionnelle les deux lois d'un anneau quelconque à l'aide du symbole + (addition) et de la juxtaposition (multiplication).

Définition 11.5 *Une application de l'anneau A vers l'anneau B est un morphisme d'anneau si et seulement*

$$\forall (x,y) \in A^2 \qquad f(xy) = f(x)f(y),\ f(x+y) = f(x) + f(y).$$

Si les anneaux sont intègres on impose de plus $f(1_A) = 1_B$.

Comme pour les morphismes de groupes on peut parler d'endomorphisme d'anneaux, d'isomorphisme d'anneaux, d'automorphisme d'anneaux.

On peut parler aussi de morphisme de corps, c'est un morphisme pour les structures d'anneaux sous-jacentes. On remarquera qu'un morphisme de corps est nécaisseremnt injectif, puis que l'image de tout élément non nul donc inversible est nécessairement inversible donc non nul.

Proposition 11.3 *Si A est un anneau unitaire l'application $n \mapsto n.1$ est un morphisme d'anneaux de $\mathbb{Z}$ vers A.*

Définition 11.6 *Si f est un morphisme d'anneau le noyau de f est le noyau du morphisme de groupes sous-jacent. On a donc*

$$\text{Ker } f = \{x; f(x) = 0\}.$$

A partir de maintenant, dans toute cette section les anneaux sont suposés commutatifs.

Définition 11.7 *Une partie I d'un anneau commutatif A est un idéal de A si et seulement si :*
- *I est uns sous-groupe de $(A,+)$,*
- *$\forall x in I\ \forall a \in A\ ax \in I$.*

Proposition 11.4 *Le noyau de tout morphisme d'anneaux est un idéal.*

Proposition 11.5 *Si x est un élément de l'anneau commutatif A alors la partie $xA = Ax = \{ax; a \in A\}$ est un idéal de A, c'est le plus petit idéal de A contenant x ; c'est l'idéal engendré par x.*

Hors-programme : un idéal de la forme Ax s'appelle un idéal principal. Un anneau commutatif intègre dans lequel tout idéal est principal s'appelle un anneau principal.

11.1.3 Divisibilité

Dans toute cette section A est un anneau intègre et commutatif.

11.1.3.1 Divisibilité dans un anneau commutatif intègre

Définition 11.8 *Si x et y sont deux éléments de l'anneauA l'élément x divise y si et seulement si il existe z tel que $y = xz$. On écrit $x|y$.*

Proposition 11.6 *Pour que x divise y il faut et il suffit que $Ay \subset Ax$.*

La relation de divisibilité est réflexive et symétrique mais elle n'est pas antisymétrique. On dit que c'est une relation de préordre.

Remarque 11.5 *On peut prouver que $x|y$ et $y|x$ si et seulement si il existe u inversible tel que $x = uy$. C'est une relation d'équivalence. On dit alors que x et y sont associés. par exemple x et y dans $\mathbb{Z}$ sont associés si et seulement si $x = \pm y$, deux éléments P et Q de $\mathbb{K}[X]$sont associés si et seulement si il existe c non nul tel que $P = cQ$. En particulier deux polynômes unitaires sont associés si et seulemnt si ils sont égaux. on verra ultérieurement l'intérêt de cette propriété.*

11.1.3.2 Divisibilité dans $\mathbb{Z}$

Proposition 11.7 *Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$ où n est entier.*

Proposition 11.8 *Deux éléments a et b de $\mathbb{Z}$ admettent un plus grand diviseur commun. On l'appelle le plus grand diviseur commun de a et b, noté $PGCD(a, b)$ ou $a \wedge b$.*

Proposition 11.9 *Deux éléments a et b de $\mathbb{Z}$ admettent un plus petit multiple commun. On l'appelle le plus petit multiple commun de a et b, noté $PPCM(a, b)$ ou $a \vee b$.*

Théorème 11.1 *(Théorème de Bézout) Si a et b sont deux entiers relatifs il existe u et v tels que $au+bv = a \wedge b$, de plus pour tout couple d'entiers u et v $a \wedge b$ divise $au + bv$. On en déduit que a et b sont premiers entre eux si et seulement si il existe u et v dans $\mathbb{Z}$ tels que $au + bv = 1$.*

Plus précisément si $a \geq 1$ et $b > 1$ sont premiers entre eux il existe u et v dans $\mathbb{N}$ avec $0 < u < b$ et $0 \leq v < a$ tels que $au - bv = 1$.

Théorème 11.2 *(Théorème de Gauss) Soit a, b et c trois entiers relatifs.*
- *Si a divise bc et est premier avec b alors il divise c.*
- *Si a est premier avec b, si a et b divisent c alors ab divise c.*

Les pgcd et les ppcm de deux entiers peuvent être calculés à l'aide d'une décomposition en facteurs premiers. On en déduit la relation

$$ab = (a \vee b)(a \wedge b)$$

si a et b sont deux entiers positifs.

11.2 $\frac{\mathbb{Z}}{n\mathbb{Z}}$

On suppose que n est un entier strictement positif.

Le cas $n = 1$, même s'il ne contredit pas les théorème qui suivent ne présente pas beaucoup d'intérêt. On aurait du supposer $n \geq 2$.

D'ailleurs si $n = 1$ alors $A = \frac{\mathbb{Z}}{n\mathbb{Z}}$ est isomorphe à $\{\overline{0}\}$ avec des lois triviales et surtout l'égalité des éléments neutres pour l'addition et la multiplication. La convention actuelle est que pour un corps les deux éléments neutres doivent être distincts. Pour les anneaux le consensus est moins établi. Si on prend comme définition d'un nombre premier (Petit Robert 2013) un nombre qui n'admet pas d'autre diviseur (entier positif) que 1 et lui-même, alors 1 est premier. Pour les mathématiciens 1 n'est pas premier car il est inversible, et par convention $\frac{\mathbb{Z}}{\mathbb{Z}}$ n'est pas un corps car ses deux éléments neutres ne sont pas distincts. Cela rend la suite cohérente. Mais il faut comprendre que cela ne dit rien de profond, simplement que les conventions des définitions sont cohérentes. La définition mathématique d'un élément premier est celle-ci : dans un anneau commutatif intègre un élément p est premier si il est non inversible et si $p|xy$ implique $p|x$ ou $p|y$. La notion de primalité est donc définie pour étendre le théorème de Gauss.

11.2.1 Structure d'anneau

Proposition 11.10 *La relation de congruence est compatible avec la multiplication. On peut donc, par passage au quotient, munir $\frac{\mathbb{Z}}{n\mathbb{Z}}$ d'une structure d'anneau commutatif. La projection canonique de $\mathbb{Z}$ sur $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est un morphisme d'anneaux.*

11.2.2 Eléments inversibles

Proposition 11.11 *Un élément $\overline{m}$ de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est inversible si et seulement si m et n sont premiers entre eux.*

Il y a donc $\phi(n)$ éléments inversibles dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

Proposition 11.12 *L'ensemble des éléments inversibles de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ forme un groupe pour la multiplication.*

D'une manière générale si A est un anneau l'ensemble A^* des élements inversibles de A est un groupe pour la multiplication.

Proposition 11.13 *L'anneau $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est un corps si et seulement si n est premier.*

On a vu qu'en général l'ensemble $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$ des éléments inversibles de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est un groupe multiplicatif, d'ordre $\phi(n)$. On en déduit que pour tout entier m premier avec n $m^{\phi(n)} \equiv 1 \bmod n$ (résultat connu sous le nom de théorème d'Euler).

Application à la cryptographie. Voir le codage RSA et la méthode du crible pour déterminer $\varphi(n)$ avec vos enseignants d'informatique.

La notion de caractéristique qui suit est hors-programme.

Proposition 11.14 *Soit A un anneau. L'application*

$$\begin{array}{rccc} c & : & \mathbb{Z} & \to & A \\ & & m & \mapsto & m.1_A \end{array}$$

est un morphisme d'anneaux. Sont noyaux est un idéal de $\mathbb{Z}$. Il est de la forme $n\mathbb{Z}$. L'entier n s'appelle la caractéristique de l'anneau A. Si $n = 0$ l'image de c est un sous-anneau de A isomorphe à $\mathbb{Z}$. Si $n > 0$ alors il existe une unique application C de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ vers A telle que $c = C \circ p$ et elle réalise un isomorphisme de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ sur un sous-anneau de A.

Proposition 11.15 *La caractéristique d'un corps est nulle où est un nombre premier. Si la caractéristique de $\mathbb{K}$ est nulle alors $\mathbb{K}$ est infini.*

La caractéristique de $\frac{\mathbb{Z}}{p\mathbb{Z}}$, où p est un nombre premier, est p. On remarquera que $\frac{\mathbb{Z}}{p\mathbb{Z}}(X)$ est un corps infini dont la caractéristique est p.

11.3 $\mathbb{K}[X]$

11.3.1 Définitions,rappels

Définition 11.9 *Une algèbre sur le corps $\mathbb{K}$ est un ensemble $\mathbb{L}$ muni de d'une loi externe . et de deux lois externe $+$ et $\times$ tels que $(\mathbb{L}, +, .)$ est un espace vectoriel, $\times$ est bilinéaire et possède un élément neutre. Bien que ce ne soit pas obligatoire on supposera aussi que $\times$ est associative, ce qui fait que $(\mathbb{L}, +, \times)$ est un anneau.*

Les exemples du programme sont $M_n(\mathbb{K})$, $L(E)$ et $\mathcal{F}(X, \mathbb{K})$. On remarquera que dans tous ces cas la multiplication est associative. Un exemple d'algèbre non-associative est l'algèbre de Lie $M_n(\mathbb{K})$ avec pour multiplication $A \times B = AB - BA$, qui hante régulièrement les sujets de concours. Elle ne possède pas d'élément unité.

Avec la notion d'algèbre viennent naturellement la notion de sous-algèbre et de morphisme d'algèbre. Une sous-algèbre contient l'élément unité et un morphisme conserve les éléments unité.

On rappelle que si $\mathbb{K}$ est un corps commutatif un polynôme P à coefficients dans $\mathbb{K}$ est une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de $\mathbb{K}$ à support fini, c'est-à-dire telle qu'il existe un entier n_0 avec $a_n = 0$ pour $n \geq n_0$. On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$. On peut munir $K[X]$ de deux lois internes et d'une loi externe qui en font une algèbre commutative sur $\mathbb{K}$.

On définit aussi le degré d'un polynôme à valeur dans $\mathbb{N} \cup -\infty$ et la valuation d'un polynôme à valeurs dans $\mathbb{N} \cup +\infty$. Nous ne rappellerons pas ici les propriétés classiques de ces fonctions.

Il existe dans $\mathbb{K}[X]$ une division euclidienne.

11.3.2 Divisibilité dans $\mathbb{K}[X]$

Théorème 11.3 *Tout idéal de $\mathbb{K}[X]$ est principal. Plus précisément tout idéal non nul est engendré par un unique polynôme unitaire.*

On peut donc transporter dans $\mathbb{K}[X]$ tous les résultats obtenus pour la divisibilité dans $\mathbb{Z}$. En particulier tout couple de polynôme possède un PGCD et un PPCM. Tout polynôme non nul se décompose de manière unique (à l'ordre des facteurs près) en un produit d'une constante et de polynômes irréductibles unitaires.

On a aussi :

Théorème 11.4 *(Théorème de Bézout pour les polynômes) Si A et B sont deux polynômes il existe U et V tels que $AU + BV = PGCD(A, B)$, de plus pour tout couple de polynômes U et V $PGCD(A, B)$ divise $AU + BV$. On en déduit que a et b sont premiers entre eux si et seulement si il existe U et V dans $\mathbb{K}[X]$ tels que $AU + BV = 1$.*

Plus précisément si $A \neq 0$ et $\deg B > 1$ sont premiers entre eux il existe U et V dans $\mathbb{K}[X]$ avec $0 \leq \deg U < \deg B$ et $\deg V < \deg A$ tels que $AU + BV = 1$.

Théorème 11.5 *(Théorème de Gauss) Soit A, B et C trois polynômes.*
- *Si A divise BC et est premier avec B alors il divise C.*
- *Si A est premier avec B, si A et B divisent C alors AB divise C.*