



Résumé de cours sur les Anneaux et les Corps

(4 pages)

I. Anneaux

Définition : Soit A un ensemble, $+$ et \cdot deux lois de composition interne définies sur A . Le triplet $(A, +, \cdot)$ est un anneau si les trois conditions suivantes sont vérifiées.

- $(A, +)$ est un groupe commutatif ;
- la loi \cdot est associative et admet un élément neutre ;
- $\forall (x, y, z) \in A^3, x(y + z) = xy + xz$ et $(x + y)z = xz + yz$. (On dit que \cdot est distributive par rapport à $+$.)

A est un anneau commutatif si la loi \cdot est commutative.

Si la loi \cdot ne possède pas d'élément neutre, on parle alors d'anneau non unitaire. Dans la suite, on ne considèrera que des anneaux unitaires (l'élément neutre de \cdot sera noté 1).

Conséquences de cette définition : $\forall x \in A, x \cdot 0 = 0 \cdot x = 0$ et $\forall y \in A, x \cdot (-y) = -(x \cdot y)$.

Définition : Soit $(A, +, \cdot)$ un anneau et $A' \subset A$. On dit que $(A', +, \cdot)$ est un sous-anneau de A si :

- $(A', +)$ est un sg de $(A, +)$;
- $1 \in A'$;
- A' est stable pour la loi \cdot .

Désormais, pour alléger les notations, les lois pour lesquelles les ensembles considérés sont des anneaux seront notées génériquement $+$ et \cdot , sauf si cela crée une ambiguïté.

Définition : Soit A et A' deux anneaux et f une application de A dans A' . On dit que f est un homomorphisme d'anneaux de A dans A' si :

- $\forall (x, y) \in A^2, f(x + y) = f(x) + f(y)$ et $f(x \cdot y) = f(x) \cdot f(y)$;
- $f(1) = 1$;

Avec plus de rigueur formelle, il faudrait distinguer les lois de A ($+_A, \cdot_A$) et celles de A' , les éléments neutres de A et ceux de A' ...

Idéal d'un anneau

Définition : Soit A un anneau et $I \subset A$. Si :

- I est un sg de A ;
- $\forall x \in A$ et $\forall y \in I, x \cdot y \in I$ ($y \cdot x \in I$) ; alors I est un idéal à gauche (à droite) de A .

Si le second point est remplacé par :

- $\forall x \in A, \forall y \in I, x \cdot y$ et $y \cdot x \in I$; alors I est un idéal bilatère de A .

Remarque : Un idéal ne contient pas nécessairement 1 (pensez aux idéaux de $\hat{\mathbb{Z}}$) et donc n'est pas nécessairement un sous-anneau de A . Un sous-anneau de A n'en est pas nécessairement un idéal (Si D

est l'ensemble des matrices carrées $n \times n$ qui sont diagonales, alors D est un sous-anneau de $(M_n(K), +, \times)$ mais ce n'en est pas un idéal car $M \times D$ n'est pas, en général, diagonale).

Proposition : Si f est un homomorphisme d'anneaux de A dans A' , alors $\text{Ker } f$ est un idéal bilatère de A .

$\text{Ker } f = \{x \in A / f(x) = 0_{A'}\}$ et f est, en particulier, un homomorphisme de groupe, il en résulte que $\text{Ker } f$ est un sg de $(A, +)$.

Soit $x \in A$ et $y \in \text{Ker } f$, alors $f(xy) = f(x)f(y) = 0.f(y) = 0$ (en notant 0 l'élément neutre de $+$ dans A') ; de même $f(yx) = f(y)f(x) = f(y).0 = 0$.

L'intérêt de la notion d'idéal est de permettre de définir celle d'anneau quotient (comme la notion de sg permettait de définir la notion de groupe quotient).

Proposition : Soit A un anneau et I un idéal bilatère de A . La relation R définie sur A par xRx' si $x' - x \in I$ est une relation d'équivalence et l'ensemble des classes, noté A/I , muni des opérations :

$$(x+I) + (y+I) = (x+y) + I \text{ et } (x+I)(y+I) = (xy) + I,$$

est un anneau.

Avant de donner la démonstration de cette proposition, observons que la définition de la multiplication des classes utilise le fait que I est un idéal bilatère de A . En effet, pour que la définition soit cohérente, il faut (et il suffit) que $\forall x' \in x+I$ et $\forall y' \in y+I$, $x'y' \in xy + I$ (la définition de la classe produit, $xy+I$, ne dépend pas des représentants des classes « facteurs » $x+I$ et $y+I$). Or $x' = x + i$, avec $i \in I$ et $y' = y + j$, avec $j \in I$, d'où $x'y' = (x+i)(y+j) = xy + iy + xj + ij$. MAIS, $iy \in I$ et $xj \in I$ car I est un idéal bilatère de A . Il en résulte que $x'y'$ est de la forme $xy + k$, où $k = iy+xj+ij \in I$. ce qui revient à dire que $x'y' \in xy+I$.

R est trivialement une relation d'équivalence sur A puisque I en est un sg.

L'addition des classes est commutative : $(x+I) + (y+I) = (x+y) + I = (y+I) + (x+I)$ puisque $x+y = y+x$ dans A .

Elle admet un élément neutre I , en effet $(x+I) + I = x + I$ puisque $I + I = I$.

Elle est associative : $((x+I) + (y+I)) + (z+I) = ((x+y) + I) + (z+I) = ((x+y)+z) + I$. Et l'associativité de $+$ dans A permet de conclure.

Soit $x+I$ une classe, alors $(-x)+I$, classe de l'opposé de x dans A , vérifie : $(x+I) + ((-x)+I) = (x+(-x))+I = I$. Conclusion $(-x)+I$ est la classe opposée de $x+I$ et $(A/I, +)$ est un groupe commutatif pour l'addition des classes.

La classe $1+I$, vérifie : $(x+I)(1+I) = (x.1)+I = x+I = (1+I)(x+I)$.

Soit $x+I$, $y+I$ et $z+I$ dans A/I . $((x+I)(y+I))(z+I) = (xy+I)(z+I) = (xy)z+I$. Mais \cdot est associative dans A , d'où l'associativité de la multiplication des classes.

Calculons $(x+I)((y+I)+(z+I)) = (x+I)((y+z)+I) = x(y+z)+I$. D'où le résultat grâce à la distributivité de \cdot par rapport à $+$ dans A .

Notion d'anneau principal

Une catégorie d'anneaux est particulièrement importante en vue des applications prévues dans le programme du CAPES (essentiellement $K[X]$, où K est un corps, et les \mathbb{Z}/p). C'est celle des anneaux principaux.

Définition : Soit A un anneau commutatif et I un idéal de A (nécessairement bilatère alors). On dit que I est un idéal principal de A , s'il existe $a \in A$ tel que, $\forall i \in I$, il existe $k \in A$, vérifiant $i = k.a$. Un tel idéal de A est dit engendré par a , on le note $\langle a \rangle$.

Définition : Soit A un anneau commutatif intègre. On dit que A est un anneau principal si tout idéal de A est principal.

L'intérêt de tels anneaux est de pouvoir y définir une notion de divisibilité de la façon suivante. Soit A un anneau principal, a et $b \in A$, $a \neq 0$, on dit que a divise b , on note $a|b$, si $\langle b \rangle \subset \langle a \rangle$.

Pour une étude détaillée des anneaux principaux et des anneaux euclidiens (qui sont principaux) voir, par exemple, l'ouvrage de F. Combes (Ch. XI), chez Bréal.

Corps

Définition : Soit $(K, +, \cdot)$ un anneau unitaire. Si, $\forall x \in K^*$, il existe $x' \in K$, tel que $x.x' = x'.x = 1$, alors $(K, +, \cdot)$ est un corps.

Si $\forall (x, x') \in K^2$, $x.x' = x'.x$, alors K est un corps commutatif.

Proposition : Si K est un corps, alors il est intègre, ie $\forall (x, y) \in K^2$, $x.y = 0 \Leftrightarrow x = 0$ ou $y = 0$.

Évident.

Dans le cas des anneaux finis on a le résultat : tout anneau intègre fini est un corps (cf. exercice 2).

Définition : Soit L un corps et $K \subset L$, K est un sous-corps de L si :

- K est un sous-anneau de L ;
- $K - \{0\}$ est stable par « passage à l'inverse ».

Définition : Soit K et K' deux corps et φ une application de K dans K' ; φ est un homomorphisme de corps si :

- $\forall (x, y) \in K^2$, $\varphi(x+y) = \varphi(x) + \varphi(y)$ et $\varphi(x.y) = \varphi(x).\varphi(y)$;
- $\varphi(1_K) = 1_{K'}$.

Remarque : tout homomorphisme de corps est injectif. En effet le noyau d'un tel morphisme est soit $\{0_K\}$ soit K (si $\text{Ker } \varphi$ contient $a \in K$, $a \neq 0_K$, alors $\forall b \in K$, $b = a.(a^{-1}.b)$ et $\varphi(b) = \varphi(a)\varphi(a^{-1}.b) = 0_{K'}$). Or $\varphi(1_K) = 1_{K'}$, donc ici $\text{Ker } \varphi = \{0_K\}$.

Définition : Soit K un corps et φ l'application de $\hat{\Gamma}$ dans K définie par : $\varphi(m) = m.1 (= 1+\dots+1$, où 1 figure m fois si $m \in \mathbb{N}$ et $-(1+\dots+1)$, où 1 figure $-m$ fois sinon). Le noyau de φ est un idéal de $\hat{\Gamma}$. Cet idéal est de la forme $c.\hat{\Gamma}$, on dit que la caractéristique de K est c .

Proposition : Soit K un corps et c sa caractéristique. Si $c \neq 0$, alors c est un entier premier.

Proposition : Soit K un corps et c sa caractéristique. On a les équivalences :

- K contient un sous-corps isomorphe à $\hat{\Gamma} \Leftrightarrow c = 0$;
- K contient un sous-corps isomorphe à $\hat{\Gamma}/c \Leftrightarrow c \neq 0$.

Il résulte de cette proposition que les corps usuels de l'Analyse et de la Géométrie (on ne parle pas des géométries sur des corps finis) sont tous de caractéristique nulle.

Constructibilité

La notion de nombre (et donc de point) constructible est liée à celle de nombre algébrique sur un corps.

Définition : Soit K un corps et L un sur-corps de K . Un nombre $\alpha \in L$ est dit algébrique sur K , s'il est racine d'une équation algébrique à coefficients non tous nuls dans K .

Proposition : Soit K un corps et L un sur-corps de K . Si $\alpha \in L$ est algébrique sur K , alors il existe un unique polynôme $P(X) \in K[X]$ tel que :

- $P(X)$ est unitaire ;
- $P(X)$ est irréductible dans $K[X]$;
- $P(\alpha) = 0$ et $\forall Q(X) \in K[X], Q(\alpha) = 0 \iff Q(X) \in \langle P(X) \rangle$.

Un tel polynôme s'appelle le polynôme minimal de α ; son degré est appelé le degré de α .

Puisque α est algébrique sur K , il existe $R(X) \in K[X]$, tel que $R(\alpha) = 0$. Alors l'ensemble des éléments de $K[X]$ qui s'annule en α est un idéal $I(\alpha)$ de $K[X]$. Cet anneau étant principal (bien connu), tout idéal l'est aussi et $I(\alpha)$ est engendré par un élément de $K[X]$ qui s'annule en α . Un tel générateur $R(X)$ est nécessairement de degré minimal car, s'il existe dans $I(\alpha)$ un polynôme $Q(X)$ de degré strictement inférieur à celui de $R(X)$, alors $R(X)$ est multiple de $Q(X)$ et il n'engendre pas $I(\alpha)$. En normalisant $R(X)$, on obtient un polynôme $P(X)$ de $K[X]$ qui s'annule en α et qui est de degré minimal. Il est unique à vérifier ces 2 propriétés. En effet s'il en existe un autre, le polynôme différence s'annule toujours en α et il est de degré strictement inférieur, d'où contradiction.

Il reste à vérifier que $P(X)$ est irréductible dans $K[X]$. Supposons que $P(X) = P_1(X) P_2(X)$ où les deux polynômes sont dans $K[X]$. alors $P(\alpha) = P_1(\alpha)P_2(\alpha) = 0 \iff P_1(\alpha) = 0$ ou $P_2(\alpha) = 0$. Si l'un des deux polynômes a un degré non nul, on aboutit à une contradiction avec le caractère minimal du degré de $P(X)$. il en résulte que $d^\circ P_1(X)$ ou $d^\circ P_2(X) = 0$ et donc que $P(X)$ est irréductible dans $K[X]$.

Théorème : Une condition nécessaire pour qu'un réel α soit constructible est que α soit algébrique sur \mathbb{Q} et que le degré de α soit une puissance de 2.

Ce théorème, dû à Wantzel, fournit un moyen efficace de montrer que certains nombres ne sont pas constructibles. Pour la démonstration de ce théorème et bien d'autres considérations sur la notion de nombres constructibles, voir l'ouvrage de J-C. Carrega, Théorie des Corps - La règle et le compas, chez Hermann, collection Formation des enseignants et formation continue.