IUFM d'Aix-Marseille
PCL1 de Mathématiques
Écrit d'Algèbre
Année 2011-2012

Résumé de cours sur les Anneaux et les Corps

Rappel : le programme officiel du concours pour la session 2010-2011 est celui des CPGE dont voici le détail.

Les notions d'anneau quotient et d'anneau principal sont hors programme.

a) Idéaux d'un anneau commutatif
Définition d'un morphisme d'anneaux, d'un isomorphisme. Noyau et image d'un morphisme d'anneaux commutatifs.
Définition d'un idéal d'un anneau commutatif A. Définition de l'idéal Ax (ou xA) engendré par un élément x de A. Dans un anneau intègre A, définition de la relation de divisibilité $x|y$. Pour que x divise y, il faut et il suffit que $Ay \subset Ax$.
b) Idéaux de $\mathbb{Z}$, anneau $\mathbb{Z}/n\mathbb{Z}$
Structure des idéaux de $\mathbb{Z}$. Application au théorème de Bézout et au théorème de Gauss. Caractérisation du PGCD et du PPCM de deux entiers.
Dans l'anneau $\mathbb{Z}$, compatibilité de la relation de congruence modulo n avec la multiplication ; anneau $\mathbb{Z}/n\mathbb{Z}$, morphisme canonique de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$. Caractérisation des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. Indicatrice d'Euler. L'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est un nombre premier. On pourra donner des exemples d'applications 'a la cryptographie.
Factorisation du morphisme de l'anneau $\mathbb{Z}$ dans un anneau A, de noyau $n\mathbb{Z}$. Définition de la caractéristique d'un corps.
c) Idéaux de $K[X]$
Dans ce paragraphe, on suppose que le corps de base K est un sous-corps de $\mathbb{C}$. Les anneaux quotients de l'anneau $K[X]$ sont hors programme.
Structure des idéaux de $K[X]$. Application au théorème de Bézout et au théorème de Gauss. Caractérisation du PGCD et du PPCM de deux polynômes.

I. Anneaux

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

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

A est un anneau commutatif si la loi . est commutative. Si la loi . ne possède pas d'élément neutre, on parle alors d'anneau non unitaire. Dans la suite, on ne considérera que des anneaux unitaires (l'élément neutre de . sera noté 1).
Conséquences de cette définition : $\forall x \in A, x.0 = 0.x = 0$ et $\forall y \in A, x.(-y) = -(x.y)$.

Définition : Soit $(A, +, .)$ un anneau et $A' \subset A$. On dit que $(A', +, .)$ est un sous-anneau de A si :
- $(A', +)$ est un sg de $(A, +)$;
- $1 \in A'$;
- A' est stable pour la loi .

Désormais, pour alléger les notations, les lois pour lesquelles les ensembles considérés sont des anneaux seront notées génériquement $+$ et ., 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 :
- $(x, y) \in A, f(x + y) = f(x) + f(y)$ et $f(x.y) = f(x).f(y)$;
- $f(1) = 1$.

Avec plus de rigueur formelle, il faudrait distinguer les lois de $A(+_A, .A)$ et celles de A', les éléments neutres de A et 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 $\forall y \in I, x.y \in I (y.x \in I)$.

alors I est un idéal à gauche (à droite) de A. Si le second point est remplacé par : $x \in A, y \in I, x.y$ et $y.x \in I$; alors I est un idéal bilatère de A.
Remarque : Un idéal ne contient pas nécessairement 1 (pensez aux idéaux de $\mathbb{Z}$) et donc n'est pas nécessairement un sous-anneau de A. Un sous-anneau de A n'en est pas nécessairement un idéal. Si $\mathcal{D}$ est l'ensemble des matrices carrées $n \times n$ qui sont diagonales, alors $\mathcal{D}$ est un sous-anneau de $(M_n(K), +, \times)$, mais ce n'en est pas un idéal.

Proposition : Si f est un homomorphisme d'anneaux de A dans A', alors Ker$f$ est un

idéal bilatère de A.
Ker$f = \{x \in A / f(x) = 0_{A'}\}$ et f est, en particulier, un homomorphisme de groupe, il en résulte que Ker$f$ est un sg de $(A, +)$. Soit $x \in A$ et $y \in$ 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 sgd permettait de définir la notion de groupe quotient).

Proposition : Soit A un anneau, et I un idéal bilatère de A. La relation $\mathcal{R}$ définie sur A par $x\mathcal{R}x'$ si $x' - x \in I$ est une relation d'équivalence et l'ensemble des classes, noté A/I, muni des opérations : $(x + I) + (y + I) = (x + y) + I$ 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 $\forall y' \in y + I$, $x'y' \in xy + I$, ce qui revient à dire que 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 $x'y' \in xy + I$.
La relation $\mathcal{R}$ 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 la loi . 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 . 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 $\mathbb{Z}/p\mathbb{Z}$). 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, $a, b \in A, a \neq 0$. On dit que a divise b, qu'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 François Combes *Algèbre et Géométrie* (Partie III ; paragraphe XI), chez Bréal.

Corps

Définition : Soit $(K, +, .)$ un anneau unitaire. Si, $\forall x \in K^*$, il existe $x' \in K$, tel que $x.x' = x'.x = 1$, alors $(K, +, .)$ 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^* est stable par « passage à l'inverse ».

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

- $\forall (x,y) \in K, \varphi(x+y) = \varphi(x) + \varphi(y)$ et $\varphi(x.y) = \varphi(x).\varphi(y)$;
- $\varphi(1) = 1$.

Remarque : Tout homomorphisme de corps est injectif. En effet, le noyau d'un tel morphisme est soit 0 soit K (si Kerφ 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 Ker$\varphi = 0_K$.

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

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 $\mathbb{Q} \Leftrightarrow$ la caractéristique de K est nulle ;
- K contient un sous-corps isomorphe à $\mathbb{Z}/p\mathbb{Z} \Leftrightarrow$ la caractéristique de K est non nulle.

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

Même si elles ne figurent plus explicitement dans le nouveau PO du concours, quelques propriétés importantes des corps finis sont à connaître (sans démonstration) :
- Tout corps fini est commutatif ;
- le cardinal de tout corps fini est de la forme p^n, où p est un entier premier et $n \in \mathbb{N}^*$;
- deux corps finis de même cardinal sont isomorphes (que pensez-vous de l'équivalent pour les groupes ? pour les anneaux ?) ;
- Un corps fini est de caractéristique non 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 $\forall Q(X) \in K[X], Q(\alpha) = 0 \Rightarrow Q(X) \in \langle P(X) \rangle$ (l'idéal de polynômes engendré par $P(X)$).

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, noté encore $R(X)$, 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 le seul à vérifier ces deux 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, $P(\alpha) = P_1(\alpha)P_2(\alpha) = 0 \Rightarrow P_1(\alpha) = 0$ 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 $\mathrm{d}^\circ P1(X)$ ou $\mathrm{d}^\circ P2(X)$ est égal à 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 P. L. Wantzel[1], 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 Jean-Claude Carrega, *Théorie des Corps - La règle et le compas*, chez Hermann, collection « Formation des enseignants et formation continue ».

[1] Pierre Laurent WANTZEL, mathématicien français, 1814-1848.

Définition : Soit $\mathcal{P}$ un plan affine euclidien, O et I deux points distincts de $\mathcal{P}$. Un point M de $\mathcal{P}$ est dit *constructible à la règle et au compas à partir des points de base O et I* si l'une des conditions suivantes est vérifiée :

- $M \in \{O, I\}$;
- M est l'intersection de deux droites définies par des points constructibles (de telles droites seront appelées *droites constructibles*) ;
- M appartient à l'intersection d'un cercle centré en un point constructible, passant par un point constructible (de tels cercles seront appelés des *cercles constructibles*) et d'une droite constructible ;
- M appartient à l'intersection de deux cercles constructibles.

Remarque : lorsque les points O et I sont définis sans ambiguïté, on parle alors plus simplement de points *constructibles à la règle et au compas*.

Théorème : Soit $\mathcal{P}$ un plan affine euclidien, O et I deux points distincts de $\mathcal{P}$. Une CNS pour qu'un point $M \in \mathcal{P}$ soit constructible à la règle et au compas, est que les coordonnées de M - dans le repère orthonormé $\{O, I, J\}$ construit à la régle et au compas - soient des nombres constructibles.