Vincent Pilaud
Kholles de mathématiques
MP* - Lycée Charlemagne - Paris

11 octobre 2005

Algèbre générale (ii) : Groupes, Anneaux, Corps
Révisions d'algèbre linéaire

1 Groupes, Anneaux, Corps, Arithmétique

1.1 Actions de groupes

On rappelle qu'une **action de groupe** est la donnée d'un groupe G, d'un ensemble X et d'un morphisme de groupes $\phi : G \to \mathfrak{S}(X)$, ou autrement dit d'une application

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, x) & \longmapsto & g \cdot x \end{array}$$

telle que

$\forall x \in X,\ e \cdot x = x$ (où e désigne l'élément neutre de G),

et $\forall x \in X, \forall g, h \in G,\ \ g \cdot (h \cdot x) = (gh) \cdot x$.

Étant donnée une action d'un groupe G sur un ensemble X, on définit les ensembles suivants :

- Si $x \in X$, l'**orbite** de x est l'ensemble $\omega(x) = \{g \cdot x \mid g \in G\}$. L'ensemble des orbites est noté Ω.
- Si $x \in X$, le **stabilisateur** de x est l'ensemble $\mathrm{Stab}(x) = \{g \in G \mid g \cdot x = x\}$.
- Si $g \in G$, l'**ensemble des points fixes** de g est l'ensemble $\mathrm{Fix}(g) = \{x \in X \mid g \cdot x = x\}$.

On rappelle l'**équation aux classes** : $\forall x \in X$, on a $|G| = |\omega(x)||\mathrm{Stab}(x)|$.

Actions de groupes finis

Exercice. [Transitivité d'une action de groupe]

Soit G un groupe agissant sur un ensemble X. On dit que cette action est **k-fois transitive** ($k \in \mathbb{N}^*$) si pour toute paire $((x_1, \dots, x_k), (y_1, \dots, y_k))$ de k-uplets d'éléments distincts de X, il existe un élément g de G tel que $\forall i \in \{1, \dots, k\}, g \cdot x_i = y_i$. Une action 1-fois transitive est plus simplement appelée action **transitive**.

1. Montrer que l'action de G sur X est transitive si et seulement si pour tout élément x de X, l'orbite de x est égale à X.

2. Soit $x \in X$. Montrer que l'action de G sur X est k-fois transitive si et seulement si elle est transitive et l'action de $\mathrm{Stab}(x)$ sur $X \setminus \{x\}$ est $(k-1)$-fois transitive.

3. Exemples : montrer que l'action canonique de $\mathfrak{S}_n$ sur $\{1, \dots, n\}$ est n-fois transitive, et que celle de $\mathfrak{A}_n$ est $(n-2)$-fois transitive.

Exercice. [Deux preuves du théorème de Sylow]

Soit p un nombre premier, α un entier et m un entier non divisible par p. Soit G un groupe fini de cardinal $p^\alpha m$. On va montrer (par deux méthodes indépendantes) que G possède au moins un sous-groupe de cardinal p^α. Un tel sous-groupe est appelé p-sous-groupe de Sylow de G.

1. Première méthode :

a. On note $\mathbb{F}_p$ le corps de cardinal p premier, $\mathrm{GL}_n(\mathbb{F}_p)$ le groupe des matrices carrées inversibles de taille n sur ce corps et $S_n(\mathbb{F}_p)$ le sous-groupe de $\mathrm{GL}_n(\mathbb{F}_p)$ formé des matrices triangulaires supérieures avec des 1 sur la diagonale. Montrer que $S_n(\mathbb{F}_p)$ est un p-sous-groupe de Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$.

b. On considère la relation binaire sur $\mathrm{GL}_n(\mathbb{F}_p)$ définie par

$$\forall A, B \in \mathrm{GL}_n(\mathbb{F}_p), \quad A\mathcal{R}B \Leftrightarrow A^{-1}B \in S_n(\mathbb{F}_p).$$

Vérifier que cette relation binaire est une relation d'équivalence sur $\mathrm{GL}_n(\mathbb{F}_p)$. Donner le cardinal de l'ensemble quotient $\Delta = \mathrm{GL}_n(\mathbb{F}_p)/\mathcal{R}$.

c. Soit G un sous-groupe de $\mathrm{GL}_n(\mathbb{F}_p)$. Montrer que l'application $\phi : G \times \mathrm{GL}_n(\mathbb{F}_p) \to \mathrm{GL}_n(\mathbb{F}_p)$ définie par $\phi(g, M) = gM$ (pour tout $(g, M) \in G \times \mathrm{GL}_n(\mathbb{F}_p)$) induit une action de G sur Δ.

d. Montrer qu'il existe un élément $\delta \in \Delta$ tel que le cardinal de $\omega(\delta)$ est premier avec p. En déduire que le stabilisateur de δ est un p-sous-groupe de Sylow de G.

e. Montrer que tout groupe de cardinal n se plonge dans $\mathrm{GL}_n(\mathbb{F}_p)$. En déduire le théorème de Sylow dans le cas général.

2. Seconde méthode :

Soit G un groupe de cardinal $p^\alpha m$. On considère l'action de G sur l'ensemble X de ses parties à p^α éléments définie par

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, (\{x_1, \ldots, x_{p^\alpha}) & \longmapsto & \{gx_1, \ldots, gx_{p^\alpha}) \end{array}$$

Montrer qu'il existe un élément x de X tel que le cardinal de $\omega(x)$ est premier avec p. En déduire que quitte à réitérer le procédé, le stabilisateur de x est un p-sous-groupe de Sylow de G.

Exercice. [p-groupes]

Soit p un nombre premier. On appelle **p-groupe** tout groupe dont le cardinal est une puissance de p.

1. Montrer que le centre d'un p-groupe n'est pas réduit à l'élément neutre.

2. En déduire qu'un groupe d'ordre p^2 est abélien.

Dénombrement : Théorème de Polya

Soit $\mathbb{X} = \{x_1, \ldots, x_n\}$ un ensemble d'objets, $\mathbb{A} = \{a_1, \ldots, a_m\}$ un ensemble de couleurs et G un sous-groupe de $\mathfrak{S}_n$. G agit sur $\mathbb{X}$ par

$$\begin{array}{ccc} G \times \mathbb{X} & \longrightarrow & \mathbb{X} \\ (g, x_i) & \longmapsto & g \cdot x_i = x_{g(i)} \end{array}$$

Un **coloriage** de $\mathbb{X}$ par $\mathbb{A}$ est une application $\phi : \mathbb{X} \to \mathbb{A}$. On note $\mathfrak{C}$ l'ensemble des coloriages de $\mathbb{X}$ par $\mathbb{A}$. Le groupe G agit sur $\mathfrak{C}$ par

$$\begin{array}{ccc} G \times \mathfrak{C} & \longrightarrow & \mathfrak{C} \\ (g, \phi) & \longmapsto & g \cdot \phi : x \mapsto \phi(g^{-1} \cdot x) \end{array}$$

Une orbite pour cette action est appelée **schéma de coloriage**.

Le but du problème est de montrer que le nombre S schémas est donné par

$$S = \frac{1}{|G|} \sum_{g \in G} |\mathbb{A}|^{\gamma(g)},$$

où $\gamma(g)$ désigne le nombre de cycles de g dans sa décomposition en cycles à supports disjoints.

Exercice. [Lemme de Burnside]

On considère un groupe G agissant sur un ensemble X. En considérant le cardinal de l'ensemble $F = \{(g, x) \in G \times X \mid g \cdot x = x\}$, montrer la formule de Burnside :

$$|G||\Omega| = \sum_{g \in G} |\mathrm{Fix}(g)|.$$

Exercice. [Théorème de Polya]

On considère l'action de G sur l'ensemble des coloriages décrite plus haut.

Soit $g \in G$. Montrer qu'un coloriage ϕ est dans $\mathrm{Fix}(g)$ si et seulement si il est constant sur les orbites de $\langle g \rangle$ pour l'action de G sur $\mathbb{X}$. En déduire une bijection entre $\mathrm{Fix}(g)$ et l'ensemble des applications de $\{1, \ldots, \gamma(g)\}$ dans A. Montrer alors la formule de Polya.

Exercice. [Application]

Quel est le nombre de colliers différents à 6 perles que l'on peut faire avec 3 couleurs ?

1.2 Commutativité et inversibilité dans des anneaux

Exercice. [Anneau d'éléments idempotents d'ordre 3]

Soit A un anneau (d'élément nul (resp. neutre) 0 (resp. 1)) dont tout élément est idempotent d'ordre 3 (ie. tel que $\forall a \in A, a^3 = a$).

1. Déterminer les éléments nilpotents de A (ie. les éléments $a \in A$ tels que $\exists n \in \mathbb{N}^*, a^n = 0$).

2. Soit $a, b \in A$ avec $b^2 = b$. En considérant l'élément $ba(1 - b)$, montrer que a et b commutent. En déduire que les carrés de A (ie. les éléments de la forme c^2 avec $c \in A$) sont dans le centre de A.

3. Montrer que A est commutatif.

Exercice. [Inversibilité de $1 - ab$]

Soit a et b deux éléments d'un anneau A. Montrer que $1 - ab$ est inversible si et seulement si $1 - ba$ l'est.

Exercice. [Anneau sans idéal non premier]

Soit A un anneau commutatif dans lequel tout idéal I est premier (ie. $\forall x, y \in A,\ xy \in I \Rightarrow x \in I$ ou $y \in I$). Montrer que A est un corps (pour inverser un élément x, on pourra considérer l'idéal engendré par x^2).

1.3 Les carrés dans les corps finis : loi de réciprocité quadratique

Exercice. [Quelques rappels sur les corps finis]

Montrer que la cardinalité d'un corps fini $\mathbb{K}$ est nécessairement de la forme $q = p^\alpha$ où p est un nombre premier et α un entier non nul. p est appelée **caractéristique** du corps $\mathbb{K}$.

Exercice. [Carrés en caractéristique 2]

Montrer que dans un corps de caractéristique 2, tout élément est un carré.

Exercice. [Carrés en caractéristique impaire - Symbole de Legendre - Réciprocité quadratique]

Soit $\mathbb{F}_p$ le corps fini à p éléments (avec $p > 2$). Étant donné $x \in \mathbb{F}_p$, le symbole de Legendre de x est défini par

$$\left(\frac{x}{p}\right) = \begin{cases} 0 & \text{si } x = 0 \\ 1 & \text{si } x \neq 0 \text{ est un carré dans } \mathbb{F}_p \\ -1 & \text{sinon} \end{cases}$$

Montrer que $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$. En déduire que $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$.

Montrer que $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. (On montrera que $p^2 - 1$ est divisible par 8. On en déduira l'existence d'une racine primitive huitième de l'unité ζ dans $\mathbb{F}_{p^2}$. On vérifiera que $\zeta + \zeta^{-1}$ est une racine carrée de 2 dans $\mathbb{F}_{p^2}$.On concluera en trouvant la condition nécessaire et suffisante pour que 2 soit un carré dans $\mathbb{F}_p$).

Dans la suite de l'exercice, on veut montrer que pour tous nombres premiers p et q,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Pour cela, on introduit la **somme de Gauss** de la manière suivante. Soit ω une racine primitive q-ième de l'unité dans $\overline{\mathbb{F}}_p$. On pose

$$S = \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) \omega^x.$$

Montrer que $S^2 = (-1)^{\frac{q-1}{2}} q$, puis que $S^{p-1} = \left(\frac{p}{q}\right)$. Conclure.

Exercice. [Une équation dans $\mathbb{F}_p$]
Soient $u, v, w \in \mathbb{F}_p \setminus \{0\}$. Montrer que l'équation $ux^2 + vy^2 = w$ admet une solution $(x, y) \in \mathbb{F}_p^2$.

1.4 Arithmétique

Exercice. [Théorème de Wilson]
Soit $n \in \mathbb{N}^*$. Montrer que n est premier si et seulement si $(n-1)! = -1 \mod n$.

Exercice. [Parité de $\sigma(n)$]
Soit $n \in \mathbb{N}^*$. On note $\sigma(n)$ la somme de ses diviseurs. Donner une condition nécessaire et suffisante pour que $\sigma(n)$ soit impair.

Exercice. [Autour des nombres de Fermat]
Soit $a \geq 2$ et $m \geq 1$ deux entiers.

1. Montrer que si $a^m - 1$ est premier, alors m est premier et a est pair. Réciproque ?

2. Montrer que si $a^m + 1$ est premier, alors m est une puissance de 2 et a est pair.

3. Le but de ce qui suit est d'étudier la réciproque de cette dernière affirmation. Pour $n \in \mathbb{N}$, on définit le $n$ième nombre de Fermat par $F_n = 2^{2^n} + 1$.

a. Montrer que F_0, F_1, F_2, F_3 et F_4 sont premiers. Montrer en revanche que F_5 est divisible par 641 (on pourra remarquer que $641 = 5^4 + 2^4 = 1 + 5.2^7$ et conclure sans effectuer le calcul de la division).

b. Montrer que si $n > m$, alors F_m divise $F_n - 2$ et en déduire que F_n et F_m sont premiers entre eux (remarquer au passage que ceci fournit une autre preuve de l'existence d'une infinité de nombres premiers).

c. Montrer que si p est un diviseur premier de F_n, alors $p = 1[2^{n+1}]$. Retrouver rapidement le facteur 641 de la question a.

2 Algèbre linéaire

Exercice. [Union de sous-espaces vectoriels]

Soit E un espace vectoriel sur un corps K infini et $(F_i)_{1\leq i\leq p}$ une famille finie de sous-espaces vectoriels de E. Le but est de montrer que si $E = \bigcup_{i=1}^{p} F_i$, alors il existe $i \in \{1, \ldots, p\}$ tel que $E = F_i$.

1. Montrer le résultat pour $p = 1$ et $p = 2$.
2. Montrer le résultat par récurrence.

Exercice. [Intersection de sous-espaces vectoriels]

Soit E un espace vectoriel de dimension n et $(F_i)_{1\leq i\leq p}$ une famille finie de sous-espaces vectoriels de E. Montrer que si $\sum_{i=1}^{p} \dim(F_i) > n(p-1)$, alors $\bigcap_{i=1}^{p} F_i \neq \{0\}$.

Exercice. [Sommes directes]

Soit E et F deux espaces vectoriels sur le même corps et $(E_i)_{i\in I}$ une famille de sous-espaces vectoriels de E. On considère l'application

$$\Psi : \left\{ \begin{array}{ccc} \mathcal{L}(E,F) & \longrightarrow & \prod_{i\in I} \mathcal{L}(E_i, F) \\ u & \longmapsto & (u_{|V_i})_{i\in I} \end{array} \right.$$

Donner une condition nécessaire et suffisante pour que Ψ soit injective (resp. surjective).

Exercice. [Inverses à gauche et à droite]

Soit E un espace vectoriel et $f \in \mathcal{L}(E)$. Montrer que

- Si il existe deux applications linéaires distinctes g et h telles que $f \circ g = f \circ h = Id$, alors il en existe une infinité non dénombrable.
- Si il existe une unique application linéaire g telle que $f \circ g = Id$, alors f est inversible d'inverse g.

Exercice. [Somme de projecteurs]

1. Soit E un espace vectoriel sur un corps de caractéristique différente de 2 et p et q deux projecteurs de E. Montrer que les assertions suivantes sont équivalentes :

i) $p + q$ est un projecteur,
ii) $pq + qp = 0$,
iii) $pq = qp = 0$.

2. Soit E un espace vectoriel de dimension finie sur un corps de caractéristique nulle et $(p_i)_{1\leq i\leq p}$ une famille finie d'endomorphismes de E tels que $\sum_{i=1}^{p} p_i = Id$. Montrer que les assertions suivantes sont équivalentes :

i) $\forall i \neq j \in \{1, \ldots, p\}, p_i p_j = 0$,
ii) $\forall i \in \{1, \ldots, p\}$, p_i est un projecteur.

3. Soit E un espace vectoriel de dimension finie sur un corps de caractéristique nulle et $(p_i)_{1\leq i\leq p}$ une famille finie de projecteurs de E. Montrer que les assertions suivantes sont équivalentes :

i) $\forall i \neq j \in \{1, \ldots, p\}, p_i p_j = 0$,
ii) $\sum_{i=1}^{p} p_i$ est un projecteur.