GROUPES ET GÉOMÉTRIE, ALGÈBRE GÉNÉRALE

JEAN-PAUL CALVI

Le thème de cette séquence correspond à deux parties du programme officiel de l'agrégation interne de mathématiques :

A) Un sous-ensemble du chapitre 4 (Groupes et géométrie). Les thèmes sont les suivants. Groupes, morphismes, sous-groupe engendré par une partie. Groupes cycliques, ordre d'un élément. Théorème de Lagrange. Image et noyau. Sous-groupe distingué (ou normal). Groupe quotient. Groupe opérant sur un ensemble, orbites. Stabilisateurs. Formule des classes. Éléments conjugués, classes de conjugaison, classes de sous-groupes conjugués. Signification géométrique des notions de conjugaison. Automorphismes intérieurs d'un groupe. Polygones réguliers et groupes diédraux. Permutations d'un ensemble fini, groupe symétrique; cycles, génération par les transpositions. Décomposition d'une permutation en produit de cycles à supports disjoints. Signature. Groupe alterné. Le programme spécifie que les diverses notions sur les groupes devront être illustrées dans des situations géométriques (par exemple isométries d'un tétraèdre régulier, d'un cube).

B) Le chapitre 2 b) qui est uniquement au programme de l'écrit. Définition (les anneaux sont unitaires par définition). Formule du binôme. Idéaux d'un anneau commutatif. Morphismes d'anneaux. Anneaux quotients. Anneaux commutatifs intègres. Anneaux principaux. Exemple des entiers de Gauss, applications (équation $x^2 + y^2 = z^2$ dans $\mathbb{Z}$). Sous-corps. Corps premier. Caractéristique d'un corps. Corps des fractions d'un anneau intègre. Éléments algébriques sur un sous-corps. Dénombrabilité du corps des nombres algébriques sur $\mathbb{Q}$. Nombres transcendants.

1. Groupes

1.1. **Groupes cycliques.**

(1) Montrer qu'à isomorphisme près il existe un et un seul groupe cyclique d'ordre $n \geq 1$. Que dire de l'image d'un groupe cyclique par un morphisme ?

(2) Montrer que tout sous-groupe d'un groupe cyclique est cyclique.

(3) Déterminer en fonction des diviseurs de n, tous les sous-groupes d'un groupe cyclique d'ordre n, tous les éléments générateurs du groupe i.e. $\{x \in G : o(x) = n\}$.

(4) Montrer que tout quotient de groupe cyclique est un groupe cyclique.

(5) Soit G un groupe abélien et H, W des sous-groupes de G. Montrer HW est un sous groupe de G et que c'est le sous-groupe engendré par la réunion de H et W. Montrer que si $G = HW$ et $H \cap W$ est réduit au neutre alors $G \simeq H \times W$. Dans ce cas on dit que G est *décomposable* (en $H \times G$). Montrer plus généralement que si on a k sous-groupes H_i, $i = 1, \ldots, k$ tels

Date: Juin 2006 / préparation à l'agrégation interne de mathématiques.

que $G = H_1H_2 \dots H_k$ et tels que pour $i = 1, \dots, k$ $(H_1H_2 \dots H_{i-1}) \cap H_i$ est réduit au neutre alors $G \simeq H_1 \times \dots H_k$.

(6) Montrer qu'un groupe cyclique d'ordre $n = st$ avec s et t premier entre eux est isomorphe au produit de deux groupes cycles d'ordres respectifs s et t. Si a est un générateur du groupe, on pourra considérer les éléments a^s et a^t, les groupes qu'ils engendrent et la question précédente. En déduire que tout groupe cyclique d'ordre n tel que la décomposition en facteurs premiers de n soit $p_1^{k_1} \dots p_k^{s_k}$ est isomorphe à un produit de groupes cycliques d'ordre $p_i^{k_i}$.

(7) Un groupe cyclique G d'ordre p^k avec p premier s'appelle un *groupe cyclique primaire*. Montrer qu'un groupe cyclique primaire n'est jamais décomposable. Pour cela on établira le lemme suivant qui sera à nouveau utilisé par la suite.

Lemme 1. *Tout sous-groupe non réduit au neutre d'un groupe cyclique primaire G d'ordre p^k contient l'élément $a^{p^{k-1}}$ où a est un générateur de G.*

Pour établir le lemme, prenant $x = a^s$ un élément de H différent du neutre, avec $s \in \{1, \dots, p^k - 1\}$ que l'on écrira $s = p^l s'$ avec p et s' premiers entre eux, on calculera $x^{p^{k-l-1}u}$ où u est choisi de telle sorte que $s'u + pv = 1$.

Les deux questions suivantes sont indépendantes et peuvent être omises dans un premier temps.

(8) Soit Z le centre d'un groupe G. Montrer que si G n'est pas abélien alors G/Z ne peut pas être cyclique.

(9) Montrer que si p est premier et G est un groupe d'ordre p^2 alors $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ ou $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

1.2. **Le théorème fondamental sur les groupes abéliens finis.** On se propose de démontrer le

Théorème 2. *Tout groupe abélien fini est isomorphe à un produit de groupes cycliques primaires.*

Soit G un groupe abélien fini. On appelle P_G l'ensemble de nombre premiers p tel qu'il existe un élément de G dont l'ordre soit une puissance de p. C'est ensemble est évidemment fini. A priori, il pourrait être vide.

(1) Montrer que P_G est non vide.

(2) Soient $p \in P_G$ et G_p l'ensemble des éléments de G dont l'ordre soit une puissance de p. Montrer que G_p est un sous-groupe de G.

(3) On suppose $P_G = \{p_1, \dots, p_s\}$ on écrit G_i à la place de G_{p_i}. Montrer que $G = G_1G_2 \dots G_s$. Pour $x \in G$ on pourra considéré le groupe cyclique engendré par x et utiliser les résultats de la partie précédente.

(4) Montrer que pour $i = 1, \dots s-1$, $(G_1G_2 \dots G_{i-1}) \cap G_i$ est réduit au neutre.

Il suit que le groupe abélien G est isomorphe au produit des G_i. Chacun de ces G_i est appelé un *p_i-groupe abélien primaire*. Pour obtenir le théorème, il reste donc à établir que tout groupe abélien primaire est isomorphe à un produit de groupes cycliques primaires.

Prenons maintenant G un p-groupe abélien primaire autrement dit un groupe abélien dont tous les éléments ont un ordre égal à une puissance du nombre premier p. Choisissons un élément $a_1 \in G$ dont l'ordre soit maximal parmi tous les éléments de G. Le groupe cyclique engendré par a_1 est noté C_1. Parmi les éléments x de G, s'il y en a, tels que $C_1 \cap \langle x \rangle$ soit réduit au neutre, on choisit a_2 dont l'ordre soit maximal et on construit ainsi le groupe cyclique C_2. Ayant construit $C_1, \ldots, C_{i-1}$ on construit C_i si c'est possible de la manière suivante : parmi tous les éléments x de G tels que $C_1 C_2 \cdots C_{i-1} \cap \langle x \rangle$ soit réduit au neutre, on en choisit un dont l'ordre soit maximal qu'on appelle a_i et qui engendre le groupe C_i. Puisque chaque étape nécessite le choix d'un élément différent de G qui est fini, le processus se termine après un nombre fini d'étapes. Supposons donc que l'on ait finalement construit C_1, C_2, …, C_r avec $C_i = \langle a_i \rangle$ et $o(a_i) = p^{\alpha_i}$. Par construction on a

$$\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_s. \tag{1.1}$$

(5) On pose $G' = C_1 C_2 \cdot C_r$. Pourquoi a-t-on $G' \simeq C_1 \times C_2 \times \cdots \times C_r$?

Nous allons montrer que $G' = G$ et cela achèvera la démonstration du théorème puisque chaque C_i est un groupe cyclique primaire.

On montre par récurrence ($n \geq 1$) la propriété $\mathcal{P}_n$: tout élément de G d'ordre p^n appartient à G'. Cela prouvera que $G \subset G'$ et conclura la démonstration du théorème.

(6) Montrer que $\mathcal{P}_1$ est vraie. Etant donné x d'ordre p on commencera par voir que $G' \cap \langle x \rangle$ n'est pas réduit au neutre.

On suppose que $\mathcal{P}_k$ est vraie pour $k = 1, \ldots, n-1$ et la montre pour $k = n$. Soit x un élément de G d'ordre p^n. On défini l'indice $j \in \{1, \ldots, r+1\}$ comme le plus grand entier tel que

$$\alpha_{j-1} \geq n > \alpha_j \tag{1.2}$$

(qui entraîne puisque la suite α_i est décroissante $\alpha_i \geq n$ pour $i = 1, \ldots, j-1$). Dans le cas où $j = r + 1$ l'inégalité de droite est supprimée. On pose $Q = C_1 C_2 \cdots C_{j-1}$.

(7) Montrer que $Q \cap \langle x \rangle$ n'est pas réduit au neutre.

Puisque $Q \cap \langle x \rangle$ est un sous-groupe du groupe cyclique primaire $\langle x \rangle$, s'il n'est pas réduit au neutre, on peut lui appliquer le lemme 1 pour déduire qu'il contient nécessairement l'élément $y = x^{p^{n-1}}$. Cet élément y appartient donc aussi à Q. Par définition de Q, on en déduit l'existence d'entier l_i tel que

$$y = a_1^{l_1} a_2^{l_2} \cdots a_{j-1}^{l_{j-1}}. \tag{1.3}$$

(8) Montrer, en utilisant l'ordre de y, que chaque $a_{i-1}^{p l_{i-1}}$ est égal au neutre. (Revoir l'argument utilisé dans la réponse de la question (5)). En déduire, en utilisant (1.2) que p^{n-1} divise l_i.

On écrit $l_i = p^{n-1} m_i$ et on pose $z = a_1^{m_1} a_2^{m_2} \cdots a_{j-1}^{m_{j-1}}$.

(9) Montrer que $(x z^{-1})^{p^{n-1}}$ est l'élément neutre.

(10) En déduire, en utilisant l'hypothèse de récurrence, que $x z^{-1}$ puis x appartiennent à G' et cela achèvera la preuve de la la validité de $\mathcal{P}_n$.

Une version plus complète du théorème fondamental précise que la décomposition est unique à l'ordre près des facteurs autrement dit si

$$G \simeq H_1 \times \cdots \times H_s \simeq W_1 \times \cdots \times W_l \tag{1.4}$$

avec les H_i et les W_i des groupes cycliques primaires alors nécessairement $l = s$ et il existe une permutation σ de $\{1,\ldots,s\}$ telle que $H_i = W_{\sigma(i)}$ et ceci pour tout $i \in \{1,\ldots,s\}$.

2. Groupes opérant sur un ensemble

2.1. **Définitions.** Soient G un groupe de neutre e et Ω un ensemble non vide. Une application Ψ de $G\times\Omega \to \Omega$ pour laquelle on note $g\cdot x := \Psi(g,x)$ est appelée une *opération* de G sur Ω si elle vérifie les deux conditions suivantes

(1) $\forall g,g' \in G\ \forall x \in \Omega\ g \cdot (g' \cdot x) = (gg') \cdot x$,

(2) $\forall x \in \Omega,\ e \cdot x = x$.

On dit alors que G *opère* sur Ω (par Ψ). Pour être précis, il faudrait parler d'opération à gauche et l'on pourrait définir de manière similaire (comment ?) une opération à droite dont l'étude ne différerait en rien. Si $\hat{g}$ désigne l'application $x \in \Omega \to g \cdot x \in \Omega$ alors (exercice) $\hat{g} \in \mathbf{S}(\Omega)$ où $\mathbf{S}(\Omega)$ est le groupe des bijections de Ω dans lui-même et l'application $g \in G \to \hat{g} \in \mathbf{S}(\Omega)$ est un morphisme de groupe (exercice). Lorsque ce morphisme est injectif, on dit que l'opération Ψ est *fidèle* ou *effective*.

2.2. **Exemples.** Les groupes les plus usuels sont déjà des groupes de fonctions sur un ensemble Ω et il y a alors une opération triviale : on applique la fonction g à l'élément x. Par exemple si G est le groupe des permutations $\mathbf{S}_n$ alors on prend $\Omega = \Omega(n) = \{1,\ldots,n\}$ et $\sigma \cdot n := \sigma(n)$. Si G est un sous-groupe de $\mathbf{GL}_n(\mathbb{K})$ (le groupe des matrices inversibles d'ordre n à coefficients dans K) alors chaque élément de G comme toute matrice s'identifie à une application linéaire sur $\mathbb{K}^n$ et l'opération de G sur $\mathbb{K}^n$ est $g \cdot x = g(x)$. Le cas suivant couvre pratiquement toutes les applications non théoriques du concept d'opération.

(1) Soit G un groupe et ϕ un morphisme de G dans $\mathbf{GL}_n(\mathbb{K}^n)$ alors l'application définie sur $G \times \mathbb{K}^n$ par $g \cdot x = \phi(g)(x)$ est une opération de G sur $\mathbb{K}^n$ (exercice). En déduire une opération de $\mathbf{S}_n$ sur $\mathbb{K}^n$.

(2) Construire à partir d'une opération de G sur Ω, une opération de G sur Ω^n.

Il est cependant souvent très commode pour étudier les groupes pour eux-mêmes d'utiliser des opérations dans le cas ou Ω est égal au groupe opérant ou, au moins, est directement construit à partir de ce groupe. Voici quelques exemples.

(3) *L'opération par translation à gauche.* On prend $\Omega = G$ et $g \cdot x = gx$ (le produit de g par x.

(4) *L'opération par conjugaison.* On prend $\Omega = G$ et $g \cdot x = gxg^{-1}$. (Exercice : vérifier que c'est bien une opération).

(5) *L'opération par conjugaison sur les sous-groupes.* On prend pour Ω l'ensemble des sous-groupes de G et si X est un de ces sous-groupes on pose $g \cdot X = gXg^{-1} = \{gxg^{-1} : x \in X\}$. (Exercice : vérifier que c'est bien une opération).

2.3. **Orbites et Stabilisateurs.** Si G opère sur Ω, on définit un relation d'équivalence (exercice) sur Ω par xRy s'il existe $g \in G$ tel que $g \cdot x = y$. Les classes d'équivalence de cette opération sont appelées *orbites*. L'orbite de $x \in \Omega$, notée $O(x)$ est ainsi donnée par

$$O(x) = \{g \cdot x \,:\, g \in G\}. \tag{2.1}$$

(1) Le groupe des rotations de centre A opère sur le plan. Décrire les orbites.

(2) Soit $\sigma \in \mathbf{S}_n$. le groupe cyclique engendré par σ opère sur Ω_n. Décrire les orbites.

(3) Le groupe $\mathbf{Is}(\mathcal{P})$ des isométries (affines) du plan opère sur $\mathcal{P}$ par $f \cdot (M,N) = (f(M),f(N))$. A quelle(s) conditions(s) deux couples (M,N) et (M',N') sont-ils sur la même orbite?

(4) Lorsque G opère sur lui-même par conjugaison, à quelle condition l'orbite de x est-elle réduite à x?

Lorsque l'opération contient une et une seul orbite, on dit que l'opération est *transitive*. Pour $x \in \Omega$, on note $Stab(x)$ l'ensemble des $g \in G$ tel que $g \cdot x = x$.

(5) Montrer que $Stab(x)$ est un sous-groupe de g.

Puisque $Stab(x)$ est un groupe, on peut définir le quotient $G/Stab(x)$ comme l'ensemble des classes d'équivalences de la relation gRg' si $g^{-1}g' \in Stab(x)$ (ce n'est pas nécessairement un groupe).

(6) On veut définir une application ϕ sur $O(x)$ par $\phi(g \cdot x) = g\,stab(x)$, autrement dit $\phi(g \cdot x)$ est la classe de g dans $G/Stab(x)$. Montrer que cette définition est consistante. (Où est le problème?) Montrer ensuite qu'elle est bijective puis les théorèmes suivants.

Théorème 3. *Si $x' = g \cdot x$ alors $stab(x') = g\,stab(x)\,g^{-1}$.*

Théorème 4. *Si Ω est fini et que l'opération de G sur Ω possède r orbites $O(x_i)$, $i = 1,\ldots,r$, alors*

$$|\Omega| = \sum_{i=1}^{r} |G/stab(x_i)| \tag{2.2}$$

où $|\cdot|$ désigne le cardinal.

2.4. **Deux applications.** Le théorème précédent est particulièrement utile pour démontrer des résultats théoriques sur les groupes finis. Les plus importants étant les théorèmes de Sylow qui ne sont pas au programme. Nous donnerons deux applications assez élémentaires.

(1) Soit G un groupe fini que l'on fait opérer sur lui-même par conjugaison (voir au dessus). Montrer que le nombre d'orbites ayant un cardinal égal à 1 est égal à $|Z(G)|$ où $|Z(G)|$ désigne le centre du groupe. En déduire une démonstration basée sur (2.2) du théorème suivant.

Théorème 5. *Si G un groupe fini de cardinal p^n où p est un nombre premier > 1 alors le centre de G n'est pas réduit à l'élément neutre.*

(2) Soit G un groupe infini et H un sous-groupe de G d'indice fini, cela signifie que $|G/H|$ est fini. On va montrer que G n'est pas simple autrement dit qu'il admet un sous-groupe propre distingué W.

On prend $\Omega = G/H$ et pour $\overline{x} \in G/H$ on pose $g \cdot \overline{x} = \overline{gx}$. Montrer que la définition est consistante et qu'elle définition une opération de G sur G/H. Prendre ensuite W comme le noyau de $g \to \hat{g}$.

3. Problème : Entiers de Gauss et équation diophantienne $x^2 + y^2 = z$

Tous les anneaux considérés sont intègres, commutatifs et unitaires.

3.1. **Les entiers de Gauss.** On note $\mathbb{Z}[i]$ le sous-ensemble de $\mathbb{C}$ défini par

$$\mathbb{Z}[i] := \{m + in \,:\, m,n \in \mathbb{Z}\}.$$

Autrement dit $\mathbb{Z}[i]$ est l'ensemble des nombres complexes dont les parties réelles et imaginaires sont des entiers.

(1) Montrer que $(\mathbb{Z}[i],+,\cdot)$ est un anneau commutatif unitaire. Cet anneau est appelé *l'anneau des entiers de Gauss*.

(2) On définit sur $\mathbb{Z}[i]$ l'application N par $N(n+im) = n^2+m^2$. Montrer que pour tous α et β dans $\mathbb{Z}[i]$, on a $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$.

(3) Montrer que si α est inversible alors $N(\alpha) = 1$.

(4) Déterminer $(\mathbb{Z}[i])^*$, le groupe des éléments inversibles de $\mathbb{Z}[i]$. Que peut-on-dire de ce groupe ?

3.2. **Arithmétique de l'anneau $\mathbb{Z}[i]$.** Un anneau A est dit *euclidien* s'il existe une application $\delta : A\setminus\{0\} \to \mathbb{N}$ telle que (1) $a,b \neq 0 \implies \delta(ab) \geq \delta(b)$ et (2) pour tous $a,b \in A$ avec $b \neq 0$, il existe q et r dans A tel que $a = qb+r$ avec $r = 0$ ou $\delta(r) < \delta(b)$.

Les anneaux $\mathbb{Z}$ et $K[X]$ où K est un corps commutatif, sont les exemples plus importants d'anneaux euclidiens.

(1) Montrer que l'application N munit $\mathbb{Z}[i]$ d'une structure d'anneau euclidien.

(2) En déduire que $\mathbb{Z}[i]$ est un anneau principal puis un anneau factoriel.

On dit qu'un anneau commutatif intègre et unitaire A est *factoriel* si tout élément $a \in A$ admet une décomposition $a = a_1 \dots a_s$ en produit d'éléments irréductibles[1] et cette décomposition est unique à l'ordre près et à la multiplication par un inversible près. On montrera que pour qu'un anneau dans lequel tout élément est décomposable en produit d'irréductible est factoriel s'il vérifie la propriété suivante : (u irréductible et $u|ab) \implies u|a$ ou $a|b$.) On montrera ensuite que tout anneau principal est factoriel.

1. Un élément est irréductible si une écriture $p = ab$ implique $a \in A^\star$ ou $b \in A^\star$, $A^\star$ désignant l'ensemble des éléments inversibles de A.

3.3. **Nombres premiers qui cessent de l'être dans $\mathbb{Z}[i]$.** Tout nombre entier premier p est élément de $\mathbb{Z}[i]$. Dans cette partie on s'intéresse à la question de savoir s'il est un élément irréductible de $\mathbb{Z}[i]$. Cela n'est pas toujours le cas comme le montre l'exemple $2 = (1+i)(1-i)$.

(1) Montrer que p premier (dans $\mathbb{N}$) est réductible dans $\mathbb{Z}[i]$ alors sa décomposition est nécessairement de la forme $p = (m+in)(m-in)$. (Utiliser la fonction N.)

(2) En déduire que si p premier est réductible dans $\mathbb{Z}[i]$ alors p est congru à 1 modulo 4. (Examiner tous les cas possibles.)

On se propose de démontrer la réciproque.

Théorème 6. *Tout nombre premier p tel que $p \equiv 1$ [4] est réductible dans $\mathbb{Z}[i]$.*

Par conséquent tout nombre premier de la forme $4k-1$ est irréductible dans $\mathbb{Z}[i]$.

(3) Démontrer le résultat suivant connu sous le nom de théorème de Wilson. (On associera chaque facteur r de $(p-1)!$ avec son associé modulo p c'est-dire le nombre s telque $rs \equiv 1$ [p].)

Théorème 7. *Soit p premier. On a $(p-1)! \equiv -1$ [p]*

(4) On passe à la démonstration du théorème 6. Soit p un nombre premier avce $p = 4k+1$, $k \in \mathbb{Z}$. On pose $t = (2k)!$.

(a) Montrer que
$$t \equiv (p-1)(p-2)\dots(p-2k) \qquad [p]$$

(b) En déduire en utilisant la définition de t, l'expression obtenue ci-dessus et la relation $p - 2k = (p+1)/2$ que
$$t^2 \equiv (p-1)! \qquad [p],$$
puis que
$$t^2 + 1 \equiv 0 \qquad [p].$$

(c) En déduire que si p est irréductible dans $\mathbb{Z}[i]$ alors p divise $t+i$ ou $t-i$ et en déduire une contradiction.

3.4. **L'équation $x^2 + y^2 = z$.**

(1) Déduire de la partie précédente le

Théorème 8. *Si p est un nombre premier positif tel que $p \equiv 1$ [4] alors il est égal à la somme de deux carrés (d'entiers).*

(2) Il nous reste à établir le

Théorème 9. *Un nombre $t \in \mathbb{Z}$ est égal à la somme de deux carrés si et seulement si chaque diviseur premier p de t de la forme $p = 4k-1$ apparaît avec un exposant pair dans la décomposition de t.*

(a) Montrer que la condition est suffisante.

(b) Nous montrons que la condition est nécessaire. Supposons donc que $t = m^2 + n^2$ et appelons p un nombre premier de la forme $p = 4k - 1$ qui apparaît dans la décomposition de t. (i) Montrer que $p|(m + in)$ ou $p|(m - in)$. (ii) En déduire que $p^2|t$ et conclure.

Laboratoire Emile Picard, Université Paul Sabatier, Toulouse