Université Denis Diderot Paris 7, Semestre septembre 2006-janvier 2007

Master 1, math-info, cours d'algèbre

Un corrigé du Partiel du 7 novembre 2006.

Le problème et les exercices sont indépendants. Les groupes et ensembles sont tous supposés finis.

Exercice 1

1.a) *Soit G un groupe possédant m (exactement) p-sous-groupes de Sylow. En faisant agir G sur ces sous-groupes, en déduire un homomorphisme non trivial $\rho : G \to \mathcal{S}_m$.*

Notons X l'ensemble des p-sous-groupes de Sylow, d'après les théorèmes de Sylow, l'action par conjugaison, $(g, P) \mapsto gPg^{-1}$ de $G \times X$ vers X est transitive et détermine donc un homomorphisme non trivial $\rho : G \to Bij(X) \cong \mathcal{S}_m$.

1.b) *Soit G un groupe de cardinal* 36, *montrer qu'il n'est pas simple. [Indication : considérer ses* 3*-sous-groupes de Sylow.]*

D'après les théorèmes de Sylow, si n_3 désigne le nombre de 3-sous-groupes de Sylow, on sait que n_3 divise 4 et que $n_3 \equiv 1 \bmod 3$, donc $n_3 = 1$ ou 4. Si $n_3 = 1$, alors il existe un unique 3-sous-groupe de Sylow qui est forcément distingué donc G n'est pas simple. Si $n_3 = 4$, on trouve d'après la question précédente un homomorphisme non trivial $\rho : G \to \mathcal{S}_4$ qui ne peut pas être injectif car 36 ne divise pas 24 donc le noyau $\operatorname{Ker} \rho$ est un sous-groupe distingué non trivial et G n'est pas simple.

Exercice 2

Soit G un groupe agissant transitivement sur un ensemble X de cardinal $d \geq 2$. On se propose de démontrer le théorème suivant :

Théorème. *Le nombre d'éléments de G agissant sans point fixe sur X est $\geq |G|/d$.*

On notera $X^g := \{x \in X \mid g \cdot x = x\}$ et f_i le nombre d'éléments de G possédant exactement i points fixes.

2.a) *Montrer que le nombre d'orbites sous l'action d'un groupe G sur un ensemble Y est donnée par la formule suivante :*

$$|G\backslash Y| = \frac{1}{|G|} \sum_{g \in G} |Y^g|$$

[Indication : on pourra compter de deux manières différentes le cardinal de l'ensemble $\{(g, y) \in G \times Y \mid g \cdot y = y\}$.]

Appelons A l'ensemble suggéré par l'indication, exprimons son cardinal de deux façons. D'une part

$$|A| = \sum_{g \in G} |\{y \in Y \mid g \cdot y = y\}| = \sum_{g \in G} |Y^g|$$

et d'autre part, en invoquant la formule des classes $|\mathcal{O}(y)| = |G|/|G_y|$, on a

$$|A| = \sum_{y \in Y} |\{g \in G \mid g \cdot y = y\} = \sum_{y \in Y} |G_y| = \sum_{y \in Y} |G|/|\mathcal{O}(y)| = |G| \sum_{y \in Y} \frac{1}{|\mathcal{O}(y)|}.$$

Mais on a aussi, en notant $\mathcal{R}$ un ensemble de représentants des orbites

$$\sum_{y \in Y} \frac{1}{|\mathcal{O}(y)|} = \sum_{y \in \mathcal{R}} \sum_{x \in \mathcal{O}(y)} \frac{1}{|\mathcal{O}(y)|} = \sum_{y \in \mathcal{R}} 1 = |\mathcal{R}| = |G\backslash Y|,$$

d'où la formule demandée.

2.b) *Dans le cas présent en déduire :*

$$|G| = \sum_{g \in G} |X^g| = \sum_{i=0}^{d} i f_i \tag{1}$$

Par hypothèse, il n'y a qu'une orbite (action transitive), et on obtient donc en regroupant les f_i éléments pour lequels $|X^g| = i$:

$$1 = |G \backslash X| = \frac{1}{|G|} \sum_{g \in G} |X^g| = \frac{1}{|G|} \sum_{i=0}^{d} i f_i.$$

2.c) *Considérons l'action de G sur $X \times X$ donnée par $g \cdot (x, x') = (g \cdot x, g \cdot x')$. Montrer que $(X \times X)^g = X^g \times X^g$ et que cette action possède au moins deux orbites distinctes. [Indication : on pourra considérer l'ensemble $\Delta := \{(x, x) \mid x \in X\}$.]*

Tout d'abord on peut écrire $(X \times X)^g$ sous la forme :

$$\{(x, x') \in X \times X \mid g \cdot (x, x') = (x, x')\} = \{(x, x') \in X \times X \mid g \cdot x = x \text{ et } g \cdot x' = x'\} = X^g \times X^g.$$

Ensuite on a $\Delta \neq X \times X$ (car $|X| = d \geq 2$ donc X contient deux éléments distincts, disons x, y et $(x, y) \notin \Delta$). Or Δ est visiblement une orbite sous l'action G, donc il y a au moins deux orbites.

2.d) *En déduire l'inégalité :*

$$\sum_{i=0}^{d} i^2 f_i \geq 2|G| \tag{2}$$

On applique la formule du point 2.a) à l'action de G sur l'ensemble $X \times X$:

$$2 \leq |G \backslash X \times X| = \frac{1}{|G|} \sum_{g \in G} |(X \times X)^g| = \frac{1}{|G|} \sum_{g \in G} |X^g|^2 = \frac{1}{|G|} \sum_{i=0}^{d} f_i i^2.$$

2.e) *Montrer que*

$$\sum_{i=0}^{d} f_i = |G|. \tag{3}$$

On partitionne les éléments de G selon leur nombre de points fixes :

$$|G| = \sum_{i=0}^{d} |\{g \in G \mid g \text{ possède } i \text{ points fixes}\}| = \sum_{i=0}^{d} f_i.$$

2.f) *En utilisant* (1), (2) *et* (3), *montrer que*

$$\sum_{i=0}^{d} (i-1)(i-d) f_i \geq |G|,$$

et en déduire $f_0 \geq |G|/d$.

On calcule

$$\sum_{i=0}^{d}(i-1)(i-d)f_i = \sum_{i=0}^{d} i^2 f_i - (d+1)\sum_{i=0}^{d} i f_i + d\sum_{i=0}^{d} f_i = \sum_{i=0}^{d} i^2 f_i - (d+1)|G| + d|G| \geq 2|G| - |G| = |G|.$$

Observons finalement que $\sum_{i=0}^{d}(i-1)(i-d)f_i = df_0 + \sum_{i=1}^{d}(i-1)(i-d)f_i \leq df_0$ parce que les autres termes sont négatifs ou nuls. On en tire bien $df_0 \geq |G|$.

Problème.

On rappelle que D_n désigne le groupe à $2n$ éléments des isométries d'un polygone régulier à n côtés. On se propose de montrer que si G est un groupe de cardinal 70 alors G est isomorphe à l'un des 4 groupes suivants

$$\mathbf{Z}/70\mathbf{Z},\ D_{35},\ D_5 \times \mathbf{Z}/7\mathbf{Z},\ D_7 \times \mathbf{Z}/5\mathbf{Z}.$$

On note $n_p = n_p(G)$ le nombre de p sous-groupes de Sylow d'un groupe G et $o(n) = o_G(n)$ le nombre d'éléments d'ordre n.

Préliminaires.

c.1) *Rappeler pourquoi un groupe de cardinal $2p$ est isomorphe à $\mathbf{Z}/2p\mathbf{Z}$ ou D_p (ici p est premier impair).*

Si $|G| = 2p$, les théorèmes de Sylow fournissent un sous-groupe distingué H de cardinal p donc isomorphe à $\mathbf{Z}/p\mathbf{Z}$ et un sous-groupe d'ordre 2 disons $K = \{e, s\}$. Soit r un générateur de H. On a nécessairement $srs^{-1} \in H$ donc égal à r^a. Comme $s^2 = e$, on voit que $r^{a^2} = r$ donc $a^2 \equiv 1 \bmod p$ et donc $a \equiv \pm 1 \bmod p$. Si $a = +1$, l'élément s commute avec r donc rs est d'ordre $2p$ et $G \cong \mathbf{Z}/2p\mathbf{Z}$. Si $a = -1$ on trouve $srs^{-1} = r^{-1}$, ce qui caractérise le groupe diédral.

c.2) *Que valent n_2 et n_p dans le cas $G = D_p$?*

On a $n_p = 1$ (il n'y a qu'un seul Sylow qui est distingué) et $n_2 = p$, en effet il y a p éléments d'ordre 2 (les symétries).

Si S et T sont deux sous-groupes de G tels que $S \cap T = \{e\}$ on considère $ST := \{xy \mid x \in S,\ y \in T\}$.

c.3) *Montrer que, si S est distingué dans G, alors $ST = TS$ est un sous-groupe de cardinal $|S|.|T|$.*

Si S est distingué, on a pour tout $t \in G$ l'égalité $St = tS$ d'où l'égalité $ST = TS$. Si $g = st$ et $g' = s't'$ alors $gg' = sts't' = s(ts't^{-1})tt' \in ST$ et $g^{-1} = t^{-1}s^{-1} \in TS = ST$ donc ST est bien un sous-groupe. Enfin il nous reste à montrer que l'application $\phi : S \times T \to G$ définie par $\phi(s,t) = st$ (dont l'image est, par définition, ST) est injective; cela nous donnera $|S|.|T| = |S \times T| = |ST|$. Supposons que $\phi(s,t) = \phi(s',t')$ alors $st = s't'$ et $(s')^{-1}s = t't^{-1}$ est donc un élément de $S \cap T$ donc vaut e et donc $s = s'$ et $t = t'$.

c.4) *Montrer que, si S et T sont distingués dans G, alors ST est un sous-groupe isomorphe à $S \times T$. En déduire qu'un groupe de cardinal 35 est cyclique.*

Calculons $sts^{-1}t^{-1} = s(ts^{-1}t^{-1}) = (sts^{-1})t^{-1}$, on voit que cet élément est dans S et T donc est trivial, ce qui signifie que s et t commutent $st = ts$. Cela entraîne que ϕ est un homomorphisme car

$$\phi((s,t) * (s',t')) = \phi(ss', tt') = ss'tt' = sts't' = \phi(s,t)\phi(s',t').$$

Ainsi dans ce cas $\phi : S \times T \to ST$ est un isomorphisme.
Si $|G| = 35$, le groupe contient un unique 5-sous-groupe de Sylow disons $S \cong \mathbf{Z}/5\mathbf{Z}$ et un unique 7-sous-groupe de Sylow disons $T \cong \mathbf{Z}/7\mathbf{Z}$; comme il sont tous les deux distingués et d'intersection triviale, d'après les questions précédentes, on voit que

$$ST \cong S \times T \cong \mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/7\mathbf{Z} \cong \mathbf{Z}/35\mathbf{Z}.$$

Enfin, ST ayant pour cardinal 35 doit être égal à G.

Classification des groupes de cardinal 70.
On revient au problème initial et on suppose maintenant que G a pour cardinal 70.

d.1) *Exprimer $o(p)$ en terme de n_p et énumérer les valeurs possibles a priori pour n_2, n_5 et n_7.*

Comme les p-sous-groupes de Sylow sont de cardinal p (pour $p = 2$, 5 ou 7) ils sont deux-à-deux disjoints hormis l'élément e bien sûr présent dans chacun d'eux. Ainsi, si $H_1, \ldots, H_{n_p}$ désigne les p-sous-groupes de Sylow, on a :

$$\left| \cup_{i=1}^{n_p} H_i \setminus \{e\} \right| = n_p(p-1).$$

Par ailleurs, d'après les théorèmes de Sylow l'ensemble du membre de gauche est égal à l'ensemble des éléments d'ordre p, donc $o(p) = n_p(p-1)$. [N.B. Cette formule devient fausse, en général, si p^2 divise $|G|$.
Toujours d'après les théorèmes de Sylow, n_5 divise 14 et est $\equiv 1 \bmod 5$ donc $n_5 = 1$ et, de même $n_7 = 1$. Quant à n_2 il doit diviser 35 et être impair donc peut *a priori* prendre les valeurs $1, 5, 7, 35$.

d.2) *Déduire de ce qui précède que G possède un sous groupe K d'ordre 35, montrer que K est distingué dans G.*

Appelons S l'unique 5-sous-groupe de Sylow et T l'unique 7-sous-groupe de Sylow, ils sont tous les deux distingués, donc $K := ST$ est un sous-groupe de cardinal 35 qui est automatiquement distingué. [On pouvait aussi remarquer que $(G : K) = 2$ donc K est distingué.]

d.3) *En déduire que G contient un sous-groupe distingué $K \cong \mathbf{Z}/35\mathbf{Z}$.*

D'après les questions précédentes, on a $K = ST \cong S \times T \cong \mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/7\mathbf{Z} \cong \mathbf{Z}/35\mathbf{Z}$.

d.4) *Calculer n_2 dans le cas des quatre groupes $\mathbf{Z}/70\mathbf{Z}$, $D_7 \times \mathbf{Z}/5\mathbf{Z}$, $D_5 \times \mathbf{Z}/7\mathbf{Z}$ et D_{35}; en déduire qu'ils ne sont pas isomorphes.*

On a $n_2(\mathbf{Z}/70\mathbf{Z}) = 1$ car le groupe est abélien; par ailleurs, si B est de cardinal impair, un 2-sous-groupe de Sylow de $A \times B$ est contenu dans $A \times \{e\}$ donc $n_2(A \times B) = n_2(A)$ et enfin on sait que, pour n impair, $n_2(D_n) = n$ puisque D_n contient n symétries d'ordre 2. On en déduit $n_2(D_7 \times \mathbf{Z}/5\mathbf{Z}) = n_2(D_7) = 7$, $n_2(D_5 \times \mathbf{Z}/7\mathbf{Z}) = n_2(D_5) = 5$ et $n_2(D_{35}) = 35$;

d.5) *Inversement, montrer en considérant les valeurs possibles de n_2 que G est isomorphe à un des 4 groupes cités.*

Cette question était plus délicate, on peut par exemple raisonner ainsi. Choisissons un générateur r de $ST = K \cong \mathbf{Z}/35\mathbf{Z}$ et s un élément d'ordre 2 et notons $R = \{e, s\}$. Observons que $srs^{-1} = r^a$ avec maintenant $a \in \mathbf{Z}/35\mathbf{Z}$ tel que $a^2 = 1$. Comme $a^2 \equiv 1 \bmod 35$ équivaut, par le lemme chinois, à $a^2 \equiv 1 \bmod 5$ et $a^2 \equiv 1 \bmod 7$, on trouve quatre solutions: $a \equiv 1 \bmod 35$ ou bien $a \equiv -1 \bmod 35$ ou bien $a \equiv 1 \bmod 5$ et $a \equiv -1 \bmod 7$ ou bien $a \equiv 1 \bmod 7$ et $a \equiv -1 \bmod 5$. Dans le premier cas R commute avec K donc $G \cong K \times R \cong \mathbf{Z}/35\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \cong \mathbf{Z}/70\mathbf{Z}$. Dans le dernier cas on reconnait la loi définissant D_{35}. Dans le deuxième cas, on voit que s commute avec S mais pas avec T. Ainsi S commute avec T et R donc avec le sous-groupe RT qui est d'ordre 14 (et, comme il est non commutatif doit être isomorphe à D_7) donc $G \cong S \times RT \cong \mathbf{Z}_5 \times D_7$. Le troisième cas se traite symétriquement.