Examen du 6 novembre 2017
2 heures

L'objectif de ce problème est de démontrer le théorème suivant, dû à Frobenius :
Soit G un groupe fini et n un diviseur de l'ordre de G. Alors le cardinal $a_n(G)$ de

$$A_n(G) := \{x \in G : x^n = 1\}$$

est un multiple de n. Dans tout le texte, p désigne un nombre premier.

1. Premiers exemples.
1.1 Ecrire la liste des groupes abeliens d'ordre p^3 non isomorphes.
1.2 Pour chacun d'eux calculer $a_p(G)$ et $a_{p^2}(G)$.

2. Groupe abelien fini.
2.1 Montrer le théorème de Frobenius si G est cyclique d'ordre une puissance de p.
2.2 Montrer le théorème de Frobenius si G est abelien d'ordre une puissance de p.
2.3 Montrer le théorème de Frobenius si G est abelien fini.

3. Résultats préliminaires.
3.1 Montrer le théorème de Frobenius pour $n = |G|$.
3.2 Nous définissons la relation binaire suivante : pour $x, y \in G$, $x \sim y$ si et seulement si x et y engendrent le même sous-groupe de G. Montrer que $\sim$ est une relation d'équivalence.
3.3 Soit $x \in G$ d'ordre k. Montrer que la classe d'équivalence de x est d'ordre $\varphi(k)$ où φ désigne la fonction indicatrice d'Euler.
3.4 Montrer que pour tout $n \geq 1$, le nombre d'éléments d'ordre n dans G est multiple de $\varphi(n)$.
3.5 Soit $n = p^\alpha s$ un diviseur de $|G|$ tel que $p^{\alpha+1}$ divise $|G|$ et p ne divise pas s. Montrer que le cardinal de $A_{np}(G) \setminus A_n(G)$ est multiple de $\varphi(p^{\alpha+1})$.
3.6 Soit $x \in G$ d'ordre mn, avec $(m, n) = 1$. Montrer qu'il existe $y, z \in G$ qui commutent tels que $x = y \cdot z$ et y (resp. z) soit d'ordre m (resp. n).

4. Cas général. Nous fixons un diviseur strict n de $|G|$ et nous supposons le théorème vrai pour tout groupe G' et tout diviseur n' de $|G'|$ tels que $n' > n$ ou $|G'| < |G|$. Soit p un diviseur premier de $\frac{|G|}{n}$, $n = p^\alpha s$, $(p, s) = 1$. Nous notons $A := A_{np}(G) \setminus A_n(G)$.
Pour tout élément $a \in G$ d'ordre $p^{\alpha+1}$, nous notons
- $\mathrm{Cent}_G(a)$ le sous-groupe de G des éléments qui commutent avec a
- $C_a = \{gag^{-1}, g \in G\}$ l'ensemble des conjugués de a et

$$S_a := \{a \cdot b : b \in \mathrm{Cent}_G(a)\,,\ b^s = 1\}, \quad S_{C_a} := \bigcup_{a' \in C_a} S_{a'}.$$

4.1 Si $A = \emptyset$, montrer que $a_n(G)$ est un multiple de n.
4.2 Nous supposons désormais $A \neq \emptyset$. Montrer que p^α divise $|A|$.
4.3 Montrer que A est la réunion disjointe des S_a, a décrivant les éléments de G d'ordre $p^{\alpha+1}$. Montrer également que A est la réunion disjointe des S_{C_a}, a décrivant les éléments de G d'ordre $p^{\alpha+1}$ à conjugaison près.
4.4 Montrer que pour tout a d'ordre $p^{\alpha+1}$, $|S_{C_a}| = |C_a| \cdot |S_a|$.
4.5 Notons k le cardinal de $\mathrm{Cent}_G(a)/\langle a \rangle$ et $m := s \wedge k$. Montrer que S_a est en bijection avec

$\{y \in \mathrm{Cent}_G(a)/\langle a\rangle | y^m = 1\}$.
4.6 Montrer qu'il existe un entier $c \geq 1$ tel que $|S_a| = cm$.
4.7 Montrer que $|S_{C_a}| = \frac{|G|cm}{kp^{\alpha+1}}$.
4.8 Montrer que s divise $|S_{C_a}|$.
4.9 En déduire le théorème de Frobenius.

5. Soit G un groupe fini et n un diviseur de $|G|$ tel que $a_n(G) = n$. Montrer que tout sous-groupe d'ordre n est distingué.

6. Soit G un groupe fini de cardinal $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, avec $p_i < p_{i+1}$ premiers et $\alpha_i \geq 1$. Nous supposons que tout sous-groupe de Sylow de G est cyclique.
6.1 Montrer par récurrence descendante que pour tout diviseur n de $|G|$ de la forme $n = p_i^{\beta_i} p_{i+1}^{\alpha_{i+1}} \dots p_r^{\alpha_r}$, nous avons $a_n(G) = n$.
6.2 En déduire que tout p_r-Sylow de G est distingué.
6.3 En déduire que G est résoluble.

7. Montrer que si $|G|$ est sans facteur carré, alors G est résoluble.

8. Soit $n \geq p$. Calculer $a_p(\mathfrak{S}_n)$ et en déduire que si t est maximal tel que $tp \leq n$, alors

$$\sum_{k=1}^{t} \frac{n!}{p^k (n-kp)! k!} \equiv -1 \ [p] \, .$$

Examen du 6 novembre 2017
2 heures

The goal of this text is to prove the following theorem due to Frobenius:

Let G be finite group and n a divisor of the order of G. Then the cardinal $a_n(G)$ of

$$A_n(G) := \{x \in G : x^n = 1\}$$

must be a multiple of n. Hereinafter, p is a prime number.

1. First examples.
1.1 Write the list of abelian groups of order p^3 up to isomorphism.
1.2 For each abelian group G of order p^3, compute $a_p(G)$ and $a_{p^2}(G)$.

2. Finite abelian group.
2.1 Prove Frobenius theorem for G a cyclic p-group (of order a power of p).
2.2 Prove Frobenius theorem for G a abelian p-group.
2.3 Prove Frobenius theorem for G finite abelian group.

3. Preliminary results.
3.1 Prove Frobenius theorem for $n = |G|$.
3.2 We define the following binary relation: for $x, y \in G$, $x \sim y$ if and only if x and y generate the same subgroup of G. Prove that $\sim$ is an equivalence relation.
3.3 Let $x \in G$ be an element of order k. Prove that the equivalence class of x has order $\varphi(k)$ where φ is Euler's totient function.
3.4 For $n \geq 1$, prove that the number of elements of order n is G must be a multiple of $\varphi(n)$.
3.5 Let $n = p^\alpha s$ be a divisor of $|G|$ such that $p^{\alpha+1}$ divides $|G|$ and p does not divided s. Prove that the cardinal of $A_{np}(G) \setminus A_n(G)$ must be a multiple of $\varphi(p^{\alpha+1})$.
3.6 Let $x \in G$ be an element of order mn, with $(m, n) = 1$. Prove that there exists $y, z \in G$ such that $y \cdot z = z \cdot y$, $x = y \cdot z$ and y (resp. z) has order m (resp. n).

4. General case. We fixe a strict divisor n of $|G|$ and we assume that Frobenius theorem holds for any group G' and any divisor n' of $|G'|$ such that $n' > n$ or $|G'| < |G|$. Let p be a prime divisor of $\frac{|G|}{n}$, $n = p^\alpha s$, $(p, s) = 1$. We denote $A := A_{np}(G) \setminus A_n(G)$.
For any element $a \in G$ of order $p^{\alpha+1}$, we denote
- $\mathrm{Cent}_G(a) = \{x \in G, xa = ax\}$ (subgroup of G)
- $C_a = \{gag^{-1}, g \in G\}$ (subset of G)

$$S_a := \{a \cdot b : b \in \mathrm{Cent}_G(a)\,,\ b^s = 1\}, \quad S_{C_a} := \bigcup_{a' \in C_a} S_{a'}.$$

4.1 If $A = \emptyset$, prove that $a_n(G)$ must be multiple of n.
4.2 From now on, we assume $A \neq \emptyset$. Prove p^α divides $|A|$.
4.3 Prove that A is the disjoint union of S_a, for $a \in G$ of order $p^{\alpha+1}$. Prove that A is the disjoint union of S_{C_a}, for $a \in G$ of order $p^{\alpha+1}$ up to conjugacy.
4.4 Prove that for all a of order $p^{\alpha+1}$, $|S_{C_a}| = |C_a| \cdot |S_a|$.

4.5 Denote k the cardinal of $\mathrm{Cent}_G(a)/\langle a\rangle$ and $m := s \wedge k$. Prove that there exists a bijection from S_a to $\{y \in \mathrm{Cent}_G(a)/\langle a\rangle | y^m = 1\}$.
4.6 Prove that there exists $c \geq 1$ such that $|S_a| = cm$.
4.7 Prove that $|S_{C_a}| = \frac{|G|cm}{kp^{\alpha+1}}$.
4.8 Prove that s divides $|S_{C_a}|$.
4.9 Deduce Frobenius theorem.

5. Let G be a finite group and n dividing $|G|$ such that $a_n(G) = n$. Prove that any subgroup of order n is normal.

6. Let G be a finite group of order $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, with $p_i < p_{i+1}$ prime numbers and $\alpha_i \geq 1$. Assume that any Sylow subgroup of G is cyclic.
6.1 Prove by decreasing induction that for any n dividing $|G|$ of the form $n = p_i^{\beta_i} p_{i+1}^{\alpha_{i+1}} \dots p_r^{\alpha_r}$, we have $a_n(G) = n$.
6.2 Deduce that any p_r-Sylow of G is normal.
6.3 Prove that G is resoluble.

7. If $|G|$ has no square factor, prove that G is resoluble.

8. Let $n \geq p$. Compute $a_p(\mathfrak{S}_n)$ and deduce the following property: if t is maximal such that $tp \leq n$, then

$$\sum_{k=1}^{t} \frac{n!}{p^k (n-kp)! k!} \equiv -1 \ [p] \, .$$

Correction succincte

1. Premiers exemples.
1.1 Les groupes abeliens d'ordre p^3 sont à isomorphisme près :

$$G_1 = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z},\ G_2 = \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z},\ G_3 = \mathbb{Z}/p^3\mathbb{Z}.$$

1.2 Nous avons

$$a_p(G_1) = a_{p^2}(G_1) = p^3,\ a_p(G_2) = p^2, a_{p^2}(G_2) = p^3,\ a_p(G_3) = p, a_{p^2}(G_3) = p^2.$$

2. Groupe abelien fini.
2.1 Si $G = \mathbb{Z}/p^r\mathbb{Z}$ et n divise $|G|$ alors $n = p^i$ avec $0 \leq i \leq r$ et $a_{p^i}(G) = p^i$ est divisible par p^i. Donc le théorè de Frobenius est vérifié si G cyclique d'ordre une puissance de p.
2.2 Si G est un groupe abelien d'ordre p^r, alors $G = \Pi_{i=1}^s \mathbb{Z}/p^{\alpha_i}\mathbb{Z}$ avec $\alpha_i \geq 0$ et et $\sum_{i=1}^s \alpha_i = r$. Ainsi pour tout $j \in \{0, \ldots, r\}$,

$$a_{p^j}(G) = \pi_{i=1}^s p^{\min\{j,\alpha_i\}}.$$

Si pour tout $i \in \{1, \ldots, s\}$, $j \geq \alpha_i$, alors $a_{p^j}(G) = p^r$ est un multiple de p^j. Sinon il existe $i \in \{1, \ldots, s\}$, tel que $\min\{j, \alpha_i\} = j$ et $a_{p^j}(G)$ est un multiple de p^j. Par conséquent le théorème de Frobenius est satisfait pour les p-groupes abeliens.
2.3 Un G groupe abelien fini est produit direct de ses sous-groupes de Sylow S_p pour p parcourant l'ensemble de diviseurs premiers de G. Ainsi en décomposant $n = \Pi_{i=1}^r p_i^{\alpha_i}$, diviseur de l'ordre de G en puissance de nombres premiers distincts, nous obtenons $a_n(G) = \Pi_{i=1}^r a_{p_i^{\alpha_i}}(S_{p_i})$. Donc le théorème de Frobenius est satisfait.

3. Résultats préliminaires.
3.1 L'ordre d'un élément divise l'ordre du groupe. Donc si $n = |G|$, $G \subset A_n(G)$, $a_n(G) = n$ est un multiple de n.
3.2 La relation binaire est reflexive, symétrique et transitive. C'est donc une relation d'équivalence.
3.3 Si $y \sim x$, alors $y \in < x >$. Donc il existe $i \in \{0, \ldots, k-1\}$ tel que $y = x^i$, avec ordre de y est égal à ordre de x, donc i premier à k. Réciproquement si $i \in \{0, \ldots, k-1\}$ premier à k alors $x^i \sim x$. Donc la classe d'équivalence de x est d'ordre $\varphi(k)$.
3.4 L'ensemble des éléments d'ordre n dans G est une réunion (éventuellement vide) des classes d'équivalence pour $\sim$ donc un multiple de $\varphi(n)$ d'après la question 3.3.
3.5 Soit $x \in A_{np}(G) - A_n(G)$. Alors $x^{sp^{\alpha+1}} = 1$ et $x^{sp^\alpha} \neq 1$. Donc x^s est d'ordre $p^{\alpha+1}$ et x est d'ordre $dp^{\alpha+1}$ avec $d|s$. Réciproquement si x est d'ordre $dp^{\alpha+1}$ avec $d|s$ alors $x \in A_{np}(G) - A_n(G)$. Ainsi $A_{np}(G) - A_n(G)$ est l'ensemble des éléments d'ordre $p^{\alpha+1}d$ pour $d|s$, donc son ordre est une somme de multiples de $\varphi(dp^{\alpha+1})$ avec $d|s$. Comme s est premier à p, $\varphi(dp^{\alpha+1}) = \varphi(d)\varphi(p^{\alpha+1})$ pour tout $d|s$. Donc l'ordre de $A_{np}(G) - A_n(G)$ est un multiple de $\varphi(p^{\alpha+1})$.
3.6 Comme $(m, n) = 1$, il existe des entiers u, v tels que $um + vn = 1$. Posons $y = x^{vn}$ et $z = x^{um}$. Ainsi $x = yz = zy$ et y (resp. z) est d'ordre m (resp. n).

4. Cas général.
4.1 D'après l'hypothèse de récurrence appliquée à $(n', G') = (np, G)$, $a_{np}(G)$ est un multiple de np donc de n. Nous avons $a_n(G) = a_{np}(G) - |A|$. Ainsi si $A = \emptyset$, $a_n(G) = a_{np}(G)$ est un multiple de n.
4.2 D'après 3.5, $|A|$ est un multiple de $\varphi(p^{\alpha+1}) = p^\alpha(p-1)$. Donc p^α divise $|A|$.
4.3 D'après 3.6, $A = \cup S_a$. De plus soit $x \in S_a \cap S_{a'}$, $x = ab = a'b'$. Comme s et $p^{\alpha+1}$ sont premiers entre eux, il existe u, v avec $su + p^{\alpha+1}v = 1$ donc $x^{su} = a = a'$. Par conséquent A est la réunion disjointe des S_a.
L'ensemble des éléments de G d'ordre $p^{\alpha+1}$ est la réunion disjointe des C_a pour a décrivant les éléments de G d'ordre $p^{\alpha+1}$ à conjugaison près. Donc A est réunion disjointe des S_{C_a}.
4.4 Soit $a \in G$ d'ordre $p^{\alpha+1}$ et $g \in G$, alors S_a et $S_{gag^{-1}}$ sont en bijection (via $(a, b) \mapsto (xax^{-1}, xbx^{-1})$)

et donc ont le même cardinal. Par conséquent $|S_{C_a}| = |C_a| \cdot |S_a|$.
4.5 La projection canonique $\mathrm{Cent}_G(a) \longrightarrow \mathrm{Cent}_G(a)/ < a >$ induit une application

$$\psi : \{b \in \mathrm{Cent}_G(a) | b^s = 1\} \longrightarrow \{y \in \mathrm{Cent}_G(a)/ < a > | y^m = 1\}$$

pour $m = (s, |\mathrm{Cent}_G(a)/ < a >))$. $\psi(b)^m = 1$. Cette application est injective car $\psi(b) = \psi(b')$ implique $b = b'a^j$, donc $a^{js} = 1$ donc $a^j = 1$ car $(s, p) = 1$. Cette application est surjective car $y \in \mathrm{Cent}_G(q)/ < a >$ avec $y^m = 1$ admet un relèvement $\tilde{y} \in \mathrm{Cent}_G(a)$ tel qu'il existe $j \in \{0, \ldots, p^{\alpha+1} - 1\}$ avec $\tilde{y}^m = a^j$. Comme $(s, p^{\alpha+1}) = 1$, il existe u, v avec $us + p^{\alpha+1}v = 1$. Notons $s = \ell m$ et $y' = ya^{-j\ell u}$. Ainsi y' relève y et $y'^s = y^{\ell m}a^{-j\ell us} = a^{j\ell}a^{-j\ell(1-p^{\alpha+1}v} = 1$.
4.6 Par induction.
4.7 D'après 4.4, $|S_{C_a}| = |C_a| \cdot |S_a|$. Or C_a est l'orbite de a sous l'action par conjugaison de G. Donc $|C_a| = |G|/|\mathrm{Cent}_G(a)|$ et $|\mathrm{Cent}_G(a)| = | < a > | \cdot |\mathrm{Cent}_G(a)/ < a > | = p^{\alpha+1}k$. Ainsi $|S_{C_a}| = \frac{|G|cm}{kp^{\alpha+1}}$.
4.8 Nous avons s divise $|G|/p^{\alpha+1}$ et $(k/m, s) = 1$, donc s divise $|S_{c_a}|$.
4.9 L'ensemble A est réunion disjointe d'ensembles de cardinaux divisibles par s (d'après 4.3 et 4.8), donc s divise $|A|$. Donc d'après 4.2, $n = p^\alpha s$ divise $|A|$. Comme $a_n(G) = a_{np}(G) - |A|$ et np divise $a_{np}(G)$, nous avons $a_n(G)$ multiple de n.

5. Soit H un sous-groupe d'ordre n. Par cardinalité, $H = A_n(G)$. Pour tout $g \in G$ $gHg^{-1} \subset A_n(G)$, donc $H = gHg^{-1}$ et H est distingué.

6.
6.1 Si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} = |G|$, alors d'après 3.1, $a_n(G) = n$. Supposons que $a_{np_i}(G) = np_i$ pour $np_i = p_i^\beta p_{i+1}^{\alpha_{i+1}} \cdots p_r^{\alpha_r}$ avec $\beta \geq 1$. Posons $n = p_i^{\beta-1}p_{i+1}^{\alpha_{i+1}} \cdots p_r^{\alpha_r} = p_i^{\beta-1}s$. Ainsi $A = A_{np_i}(G) - A_n(G) \neq \emptyset$ car A_{np_i} contient un élément d'ordre p^β. Nous avons $a_n(G) = \lambda n$, $a_{np_i} = np_i$, $|A| = \mu p_i^{\beta-1}(p_i - 1)$ multiple non nul de $\varphi(p_i^\beta)$. Ainsi $sp_i^\beta = \lambda s p_i^{\beta-1} + \mu p_i^{\beta-1}(p_i - 1)$. Les facteurs premiers de s sont $p_j > p_i$ donc s divise μ donc $p_i = \lambda + \nu(p_i - 1)$. Donc $\nu = 1$ et $\lambda = 1$ donc $a_n(G) = n$.
6.2 D'après 6.1 $a_{p_r^{\alpha_r}}(G) = p_r^{\alpha_r}$. Ainsi d'après 5, tout p_r-Sylow de G est distingué.
6.3 Par induction sur le nombre de facteurs premiers distincts, vu que le p_r-Sylow S_{p_r} est cyclique et normal, S_{p_r} et G/S_{p_r} sont résolubles. Donc G est résoluble.

7. Si $|G|$ est sans facteur carré, $|G| = p_1 \cdots p_r$ est produit de nombres premiers distincts. Ces sous-groupes de p_i-Sylow sont d'ordre p_i donc cyclique et d'après 6.3, G est résoluble.

8. Les élélements d'ordre p de $\mathfrak{S}_n$, sont les produits d'au plus t cycles de longueur p disjoints. Pour $1 \leq k \leq t$, il y a $\frac{n!}{p^k(n-kp)!k!}$ produits de k p-cycles (en effet il s'agit du cardinal de l'orbite de σ produit de k p-cycles sous l'action de $\mathfrak{S}_n$ par conjugaison, donc $|\mathfrak{S}_n|/|\mathrm{Stab}\sigma|$). Donc

$$a_p(G) = 1 + \sum_{k=1}^{t} \frac{n!}{p^k(n-kp)!k!}$$

D'après le théorème de Frobenius, p divise $a_n(\mathfrak{S}_n)$. D'où

$$\sum_{k=1}^{t} \frac{n!}{p^k(n-kp)!k!} \equiv -1 \ [p] \, .$$