Groupes et géométrie, feuille 11

N. Perrin

À rendre le mercredi 29.04.2020

Correction le mardi 30.04.2020

Exercice 1 (20 Points) Soient p et q deux nombres premiers et G un groupe d'ordre p^2q. On suppose que $p^2 - 1$ n'est pas divisible par q et que $q - 1$ n'est pas divisible par p. Montrer que G est abélien.

Solution. Soient n_p et n_q le nombre de p- et q-sous-groupes de Sylow de G.

On sait que n_p divise q et que $n_p \equiv 1 \pmod p$. Ainsi $n_p = 1$ ou $n_p = q$ mais comme p ne divise pas $q - 1$ le second cas est impossible et $n_p = 1$. Il existe donc un unique p-sous-groupe de Sylow G_p qui est distingué dans G.

On sait que n_q divise p^2 et que $n_q \equiv 1 \pmod q$. Ainsi $n_q = 1$, $n_q = p$ ou $n_q = p^2$ mais comme q ne divise pas $p^2 - 1$ le dernier cas est impossible. De plus si q divise $p - 1$ alors il divise $(p - 1)(p + 1) = p^2 - 1$ ce qui est impossible donc le deuxième cas est impossible. On a donc $n_q = 1$. Il existe donc un unique q-sous-groupe de Sylow G_q qui est distingué dans G.

On a alors $G_p \cap G_q = \{1\}$ car un élément de cette intersection a un ordre qui divise p^2 et q donc est d'ordre 1. Ainsi, on a $G = G_pG_q$ avec les deux sous-groupes distingué. Par une propriété du cours, on doit avoir un isomorphisme $G \simeq G_p \times G_q$. Comme G_p est un groupe d'ordre p^2 par un autre résultat du cours, on a que G_p est commutatif (isomorphe à $Z/p^2\mathbb{Z}$ ou $(\mathbb{Z}/p\mathbb{Z})^2$) et comme G_q est d'ordre q, il est isomorphe à $\mathbb{Z}/q\mathbb{Z}$ et est aussi commutatif. On en déduit que $G_P \times G_q$ est commutatif et donc G est commutatif. ∎

Exercice 2 (20 Points) Soient p et q deux nombres premiers distincts. Montrer qu'il n'existe pas de groupe simple d'ordre p^2q.

Solution. Soient n_p et n_q le nombre de p- et q-sous-groupes de Sylow de G. On va distinguer les cas $p > q$ et $p < q$.

Si $p > q$, alors $n_p = 1$ ou $n_p = q$ et $n_p \equiv 1 \pmod p$. Comme $q < p$, le second cas est impossible et $n_p = 1$, il existe un unique p)sous-groupe de Sylow qui est distingué et G n'est pas simple.

Si $p < q$, alors n_q divise p^2 et que $n_q \equiv 1 \pmod q$. Ainsi $n_q = 1$, $n_q = p$ ou $n_q = p^2$ mais comme $p < q$, le deuxième cas est impossible. On a donc $n_q = 1$ ou $n_q = p^2$. Si $n_q = 1$, le groupe G n'est pas simple. Sinon, on doit avoir $n_q = p^2$. Deux q-sous-groupes de Sylow ne peuvent se rencontrer que selon l'élément neutre (ar ils ont q éléments). On obtient ainsi $n_q(q - 1) = p^2(q - 1)$ éléments d'ordre q. Il reste donc $p^2q - p^2(q - 1) = p^2$ éléments qui ne sont pas d'ordre q. Comme il existe un p-sous-groupe de Sylow, ces éléments sont tous dans ce sous-groupe qui doit être unique et $n_p = 1$, le groupe G n'est pas simple. ∎

Exercice 3 ($4 \times 10 = 40$ Points) Soit G un groupe d'ordre 399.

(i) Montrer que G admet un unique 19-Sylow P qui est distingué dans G.

(ii) Soit Q un 7-Sylow. Montrer que $N = PQ$ est un sous-groupe d'ordre 133 de G et que ce groupe est cyclique.

(iii) On suppose que Q n'est pas distingué dans G. Montrer que G admet 57 sous-groupes cycliques d'ordre 133 distincts deux à deux. Quel serait le nombre d'éléments d'ordre 133 dans G ? Aboutir à une contradiction. En déduire que Q est distingué dans G et que N est distingué dans G.

(iv) Montrer que $G = NR$, où R est un 3-Sylow. En déduire que G est isomorphe au produit semi-direct d'un groupe cyclique d'ordre 133 par un groupe cyclique d'ordre 3.

Solution. On a $|G| = 399 = 3 \times 7 \times 19$

(i) Soit n_{19} le nombre de 19-sous-groupes de Sylow. On a que n_{19} divie $21 = 3 \times 7$ et que $n_{19} \equiv 1 \pmod{19}$. La seule possibilité est $n_{19} = 1$. On a donc un unique 19-sous-groupe de Sylow P qui est distingué dans G.

(ii) Soit Q un 7-sous-groupe de Sylow. Comme N est distingué dans G, l'ensemble $N = PQ$ est un sous-groupe de G. De plus, on a que $P \cap Q = \{1\}$. En effet, un element de l'intersection est d'ordre un diviseur de 7 et de 19 donc d'ordre 1. On a donc $|N| = |PQ| = |P| \cdot |Q|/|P \cap Q| = 19 \times 7 = 133$. On sait déjà que P est distingué dans N. De plus le nombre et 7-sous-groupes de Sylow de N est égal à 1 ou 19 et est congru à 1 modulo 7. Ce ne peut être que 1 est donc Q est l'unique 7-sous-groupe de Sylow de N. Ainsi par un résultat du cours, on a $N \simeq P \times Q$ comme groupe. Comme P est d'ordre 19, on a $P \simeq \mathbb{Z}/19\mathbb{Z}$, de même $Q \simeq \mathbb{Z}/7\mathbb{Z}$ donc $N \simeq \mathbb{Z}/19\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \simeq \mathbb{Z}/133\mathbb{Z}$ (par le théorème des restes chinois).

(iii) Si Q n'est pas distingué dans G, alors G admet plusieurs 7-sous-groupes de Sylow. Soit n_7 leur nombre. On a que n_7 divise $19 \times 3 = 57$ et est congru à 1 modulo 7. La seule possibilité autre que $n_7 = 1$ est $n_7 = 57$. Notons $Q_1, \cdots, Q_{57}$ ces groupes, les groupes $N_1 = PQ_1, cdots, N_{57} = PQ_{57}$ sont cycliques d'ordre 133 par la question (ii). Comme chacun de ces groupes N_i ne contient qu'un seul 7-Sylow Q_i, ces groupes qoivent être distincts. Ainsi un élément d'ordre 133 d'un de ces groupes ne peut être dans un autre. Dans chacun des N_i, il y a $\varphi(133) = (7-1) \times (19-1) = 6 \times 18 = 108$ éléments d'ordre 133 ce qui nous fait 57×108 éléments d'ordre 133 dans G, c'est bien trop ! Ainsi il n'existe qu'un 7-sous-groupe de Sylow Q qui est distingué dans G.

(iv) On a que P et Q sont distingués donc $N = PQ$ est distingué dans G. Soit R un 3-sousgroupe de SYlow. On doit avoir $N \cap R = \{1\}$ car les éléments de cet intersection sont d'ordre divisant 3 et 133 donc d'ordre 1. On a donc $|NR| = 133 \times 3 = 399 = |G|$ et $G = NR$. Par un résultat du cours, le groupe G est donc produit semi-direct de N et R. ∎

Exercice 4 (20 Points) Soit G un groupe fini et p un facteur premier de $|G|$. Soit $S \subset G$ un sous-groupe de Sylow et soit $N_G(S)$ le normalisateur de S dans G. Montrer que le nombre de p-sous-groupes de Sylow est $[G : N_G(S)]$.

Solution. Soit X l'ensemble des p-sous-groupes de Sylow. On peut faire agir G sur X par conjugaison et on sait que G agit transitivement c'est-à-dire que si $S \in X$, on a $X = G \cdot S$. Par la formule des classes, on a $|X| = |G|/|G_S| = [G : G_S]$ où G_S est le stabilisateur de S. Par ailleurs, on a

$$G_S = \{g \in G \mid g \cdot S = S\} = \{g \in G \mid gSg^{-1} = S\} = N_G(S),$$

ce qui montre le résultat. ■