Enoncés : Michel Emsalem,
Corrections : Pierre Dèbes

Théorème de Sylow

Exercice 1

Soient G un groupe fini et H un sous-groupe distingué de G. Montrer que si H et G/H sont des p-groupes, il en est de même de G.

Indication ▼ [002190]

Exercice 2

Soit G un p-groupe et H un sous-groupe distingué de G. Montrer que $H \cap Z(G)$ n'est pas réduit à l'élément neutre.

Correction ▼ [002191]

Exercice 3

Soit G un p-groupe d'ordre p^r.

(a) Montrer que pour tout entier $k \leqslant r$, G possède un sous-groupe distingué d'ordre p^k.

(b) Montrer qu'il existe une suite $G_0 = \{1\} \subset G_1 \subset \ldots \subset G_r = G$ de sous-groupes G_i distingués d'ordre p^i $(i = 1, \ldots, r)$.

(c) Montrer que pour tout sous-groupe H de G d'ordre p^s avec $s < r$, il existe un sous-groupe d'ordre p^{s+1} de G qui contient H.

Indication ▼ Correction ▼ [002192]

Exercice 4

Soit G un groupe d'ordre $2p$, où p est un nombre premier supérieur ou égal à 3. Montrer que G contient un unique sous-groupe H d'ordre p et que ce sous-groupe est distingué. Vérifier que les seuls automorphismes d'ordre 2 d'un groupe cyclique d'ordre p sont l'identité et le passage à l'inverse. En déduire que le groupe G est soit cyclique, soit non commutatif, auquel cas il possède deux générateurs s et t vérifiant les relations $s^p = 1$, $t^2 = 1$ et $tst^{-1} = s^{-1}$.

Correction ▼ [002193]

Exercice 5

Soit G un groupe non commutatif d'ordre 8.

(a) Montrer que G contient un élément a d'ordre 4 et que le sous-groupe H de G engendré par a est distingué dans G.

(b) On suppose ici qu'il existe un élément b de $G \setminus H$ qui est d'ordre 2. Soit K le sous-groupe engendré par b. Montrer que dans ce cas G est isomorphe au produit semi-direct de H par K, le générateur b de K agissant sur H via l'automorphisme $x \to x^{-1}$. Le groupe est alors isomorphe au groupe diédral D_4.

(c) Dans le cas contraire, soit b un élément d'ordre 4 de G n'appartenant pas à H. Montrer que a^2 est le seul élément d'ordre 2 de G, que le centre $Z(G)$ de G est égal à $\{1, a^2\}$. On pose $-1 = a^2$. Montrer que a et b vérifient les relations suivantes : $a^2 = b^2 = -1$, $bab^{-1} = a^{-1}$. Enfin on pose $ab = c$. Vérifier les relations suivantes :

$$a^2 = b^2 = c^2 = -1 \quad ab = -ba = c \quad bc = -cb = a \quad ca = -ac = b$$

(l'écriture $-x$ signifiant ici $(-1)x$). Ce dernier groupe est le groupe des quaternions.

Correction ▼ [002194]

Exercice 6

Montrer que le groupe diédral D_6 est isomorphe au produit direct $\mu_2 \times S_3$.

Indication ▼ [002195]

Exercice 7

(a) Soit G un groupe non abélien d'ordre 12. Soit H un 3-Sylow de G. On considère le morphisme $\theta : G \to S_{G/H}$ correspondant à l'action de G par translation de G sur G/H. Montrer que ce morphisme n'est pas injectif si et seulement si H est distingué dans G. En déduire que si H n'est pas distingué dans G, le groupe G est isomorphe à A_4.

(b) On suppose que G n'est pas isomorphe à A_4. Montrer qu'alors G admet un unique 3-Sylow $H = \{1, a, a^2\}$. Montrer ensuite que si G contient un élément b d'ordre 4, a et b vérifient les relations :

$$a^3 = b^4 = 1 \quad bab^{-1} = a^2 = a^{-1}$$

Montrer que dans le cas contraire $G \simeq D_6$.

(c) Donner la liste des classes d'isomorphisme de groupes d'ordre 12.

Correction ▼ [002196]

Exercice 8

Soient G un groupe et H un sous-groupe distingué de G. On se donne un nombre premier p et l'on suppose que H admet un unique p-Sylow S. Montrer que S est distingué dans G.

Indication ▼ [002197]

Exercice 9

Soient G un groupe et H un sous-groupe distingué de G. On se donne un nombre premier p et un p-Sylow P de G. Montrer que $H \cap P$ est un p-Sylow de H et que HP/H est un p-Sylow de G/H.

Correction ▼ [002198]

Exercice 10

Montrer qu'un groupe d'ordre 200 n'est pas simple.

Correction ▼ [002199]

Exercice 11

Pour p un nombre premier, déterminer le nombre de p-sous-groupes de Sylow du groupe symétrique S_p.

Correction ▼ [002200]

Exercice 12

(a) Donner l'ensemble $\mathscr{D}$ des ordres possibles des éléments du groupe alterné A_5 et pour chaque $d \in \mathscr{D}$, indiquer le nombre d'éléments de A_5 d'ordre d.

(b) Montrer que, pour $d = 2$ et $d = 3$, les éléments d'ordre d sont conjugués, et que les sous-groupes d'ordre 5 sont conjugués.

(c) Déduire une preuve de la simplicité de A_5.

Indication ▼ [002201]

Exercice 13

Déterminer les sous-groupes de Sylow du groupe alterné A_5.

Indication ▼ Correction ▼ [002202]

Exercice 14

Soit G un groupe simple d'ordre 60.

(a) Montrer que G admet 6 5-Sylow, et que l'action de conjugaison sur ses 5-Sylow définit un morphisme injectif $\alpha : G \to S_6$, une fois une numérotation des 5-Sylow de G choisie. Montrer que l'image $\alpha(G) = H$ est contenue dans A_6.

(b) On considère l'action de A_6 par translation à gauche sur l'ensemble $A_6/.H$ des classes à gauche. Montrer qu'elle définit un isomorphisme $\varphi : A_6 \to A_6$, une fois une numérotation des éléments de $A_6/.H$ choisie.

(c) Montrer que $\varphi(H)$ est le fixateur de la classe de l'élément neutre H, et en conclure que $G \simeq A_5$.

Correction ▼ [002203]

Exercice 15

Soient $p < q$ deux nombres premiers distincts et G un groupe d'ordre pq. Montrer que G admet un unique q-Sylow Q qui est distingué et que $G = QP$, où P est un p-Sylow de G. Montrer que G est isomorphe au produit semi-direct d'un groupe cyclique d'ordre q par un groupe cyclique d'ordre p. Montrer que si $q-1$ n'est pas divisible par p, ce produit semi-direct est en fait un produit direct.

Indication ▼ [002204]

Exercice 16

Montrer qu'un groupe d'ordre 35 est cyclique.

Indication ▼ [002205]

Exercice 17

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.

Correction ▼ [002206]

Exercice 18

Soient p et q deux nombres premiers. Montrer qu'il n'existe pas de groupe simple d'ordre p^2q.

Indication ▼ Correction ▼ [002207]

Exercice 19

Soit G un groupe d'ordre 399.

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

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

(c) 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.

(d) 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.

Correction ▼ [002208]

Exercice 20

Soit G un groupe simple d'ordre 60.

(a) Montrer que G n'admet pas de sous-groupe d'ordre 20.

(b) Montrer que si G admet un sous-groupe K d'ordre 12, alors K admet 4 3-Sylow.

(c) Montrer que si H et K sont deux sous-groupes distinct d'ordre 4 de G alors $H \cap K = \{1\}$.

(d) Montrer que si H est un 2-Sylow, alors $H \neq \mathrm{Nor}_G(H)$.

(e) Montrer que G possède 5 2-Sylow.

(f) Conclure en considérant l'action de G par conjugaison sur les 5-Sylow.

Indication ▼ [002209]

Indication pour l'exercice 1 ▲

$|G| = |G/H|\,|H|$.

Indication pour l'exercice 3 ▲

Pour les trois énoncés (a), (b) et (c), raisonner par récurrence sur r en utilisant le fait que le centre d'un p-groupe n'est pas trivial.

Indication pour l'exercice 6 ▲

On a

$$D_6 = \mathbb{Z}/6\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \simeq (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}) \simeq \mu_2 \times S_3$$

Le premier isomorphisme est une application standard du lemme chinois. Pour le deuxième, noter que le premier $\mathbb{Z}/2\mathbb{Z}$ est dans le centre du groupe et donc que l'action sur lui par conjugaison du second $\mathbb{Z}/2\mathbb{Z}$ est triviale. L'isomorphisme $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \simeq S_3$ est classique.

Indication pour l'exercice 8 ▲

Pour tout $g \in G$, gSg^{-1} est un p-Sylow de $gHg^{-1} = H$ et donc $gSg^{-1} = S$.

Indication pour l'exercice 12 ▲

Pour le (c), pour $H \neq \{1\}$ sous-groupe distingué de A_5, raisonner sur les éléments d'ordre 2, 3 et 5 contenus dans H.

Indication pour l'exercice 13 ▲

L'identification de chacun des p-Sylow ne pose pas de difficulté. Observer ensuite que les sous-groupes de Sylow sont deux à deux d'intersection réduite à $\{1\}$ et determiner leur nombre en comptant les éléments d'ordre 2, 3 et 5.

Indication pour l'exercice 15 ▲

Les théorèmes de Sylow montrent qu'il n'y a qu'un seul q-Sylow, nécessairement distingué. La suite est standard. Pour le dernier point, utiliser que $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \simeq (\mathbb{Z}/q\mathbb{Z})^\times$ (exercice **??**) et donc que $\mathbb{Z}/p\mathbb{Z}$ ne peut agir non trivialement sur $\mathbb{Z}/q\mathbb{Z}$ que si p divise $q-1$.

Indication pour l'exercice 16 ▲

D'après l'exercice 15, un groupe d'ordre 35 est isomorphe à $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$, lequel est isomorphe au groupe cyclique $\mathbb{Z}/35\mathbb{Z}$ par le lemme chinois.

Indication pour l'exercice 18 ▲

Soit G un groupe d'ordre p^2q qu'on suppose simple. On distinguera deux cas : $p > q$ et $p < q$. Dans le premier, montrer que G admet q p-Sylow d'ordre p^2 et que l'action par conjugaison de G sur les p-Sylow définit un morphisme injectif $G \hookrightarrow S_q$ et aboutir à une contradiction. Dans le second, raisonner sur le nombre de q-Sylow pour aboutir à une contradiction (on sera notamment amené à éliminer le cas $p = 2$ et $q = 3$).

Indication pour l'exercice 20 ▲

(a) Si K est un sous-groupe d'ordre 20, K a un seul 5-Sylow L et donc $K \subset \mathrm{Nor}_G(L)$ ce qui entraine que l'ordre de $\mathrm{Nor}_G(L)$ est 20 ou 60. Mais alors il y aurait 1 ou 3 5-Sylow dans G. Or 1 est impossible car G est simple et 3 contredit les prédictions du théorème de Sylow.

(b) Si K a un unique 3-Sylow L, $K \subset \mathrm{Nor}_G(L)$, et donc l'ordre de $\mathrm{Nor}_G(L)$ serait 12 ou 60. Il y aurait alors 5 ou 1 3-Sylow dans G. Comme ci-dessus, c'est impossible.

(c) Supposons que $H \cap K =< a >$ soit d'ordre 2. Le centralisateur $\mathrm{Cen}_G(a)$ de a contient H et K, donc $H \cup K$. Son ordre est au moins 6 et est divisible par 4. Les seules possibilités sont 12, 20, 60 :
- 60 est impossible, car $< a >$ serait distingué dans G
- 20 est impossible, d'après la question (a)
- 12 est impossible, car $\mathrm{Cen}_G(a)$ aurait 4 3-Sylow d'après la question (b). Il ne resterait de la place que pour un seul 2-Sylow ce qui contredit $H \cup K \subset \mathrm{Cen}_G(a)$.

(d) Si $H = \mathrm{Nor}_G(H)$, il y a 15 2-Sylow, et donc 46 éléments d'ordre une puissance de 2. Or il y a 6 5-Sylow d'intersections deux à deux triviales, et donc 24 éléments d'ordre 5. L'inégalité $46+24 > 60$ fournit une contradiction.

(e) Si H est un 2-Sylow, l'ordre de $\mathrm{Nor}_G(H)$ est 12, 20 ou 60. Mais 20 est exclu (question (a)) de même que 60 (G est simple). La seule possibilité est 12 ; il y a donc 5 2-Sylow.

(f) L'action de G par conjugaison sur les 5-Sylow fournit un morphisme $c : G \to S_5$ qui est injectif (car G est simple). Le groupe G est donc isomorphe à son image $c(G)$ qui est un sous-groupe d'ordre 60, donc d'indice 2 dans S_5. C'est donc A_5.

Correction de l'exercice 2 ▲

Le sous-groupe $H \subset G$ étant distingué, G agit par conjugaison sur H. Comme G est un p-groupe, H l'est aussi et les orbites non triviales de cette action sont de longueur divisible par p. On déduit que la réunion des orbites triviales, c'est-à-dire l'ensemble $H \cap Z(G)$ des points fixes, est aussi de cardinal divisible par p. Comme il contient l'élément neutre, il contient au moins p éléments et n'est donc pas réduit à l'élément neutre.

Correction de l'exercice 3 ▲

(a) Soit G un p-groupe d'ordre p^r. Son centre $Z(G)$ est un p-groupe non trivial. Soit $x \in Z(G) \setminus \{1\}$. Si $p^\nu > 0$ est son ordre, alors $x^{p^{\nu-1}}$ est d'ordre p et dans $Z(G)$; on peut donc supposer que x lui-même est d'ordre p. Le groupe $< x >$ est distingué dans G et le groupe quotient $G/ < x >$ est d'ordre p^{r-1}. Par hypothèse de récurrence, pour tout $k \leqslant r$, le groupe $G/ < x >$ possède un sous-groupe distingué $\mathscr{H}$ d'ordre p^{k-1}. Soit H le sous-groupe image réciproque de $\mathscr{H}$ par la surjection canonique $G \to G/ < x >$. Le sous-groupe H, image réciproque par un morphisme d'un sous-groupe distingué, est distingué dans G et $\mathscr{H} = H/ < x >$, ce qui donne $|H| = |\mathscr{H}|\,| < x > | = p^k$.

Correction de l'exercice 4 ▲

Comme p divise $|G|$, il existe dans G un élément s d'ordre p. Le sous-groupe $H =< s >$, d'indice 2, est nécessairement distingué dans G. Il est de plus le seul sous-groupe d'ordre p (cf l'exercice **??**).

De façon générale, un automorphisme χ d'un groupe cyclique $< \zeta >$ d'ordre p est déterminé par $\chi(\zeta) = \zeta^{i_\chi}$ et cet automorphisme est d'ordre 2 si et seulement si $i_\chi^2 \equiv 1$ [mod p], c'est-à-dire si $\chi(\zeta) = \zeta$ ou $\chi(\zeta) = \zeta^{-1}$ ce qui correspond aux deux automorphismes "identité" et "passage à l'inverse" (que p soit premier n'intervient pas ici ; le résultat est valable pour tout entier $p \geqslant 1$).

Soit $t \in G$ d'ordre 2 (qui existe car 2 divise $|G|$). La conjugaison par t induit un automorphisme du sous-groupe distingué H. D'apès ce qui précède, on a $tst^{-1} = s$ ou bien $tst^{-1} = s^{-1}$. Dans le premier cas, la correspondance $(s^i, t^\varepsilon) \to s^i \cdot t^\varepsilon$ ($i = 0, 1, 2$ et $\varepsilon = \pm 1$) induit un morphisme entre le produit direct $< s > \times < t >$ et G, lequel est injectif (car $< s > \cap < t >= \{1\}$) et donc est bijectif (puisque les groupes de départ et d'arrivée ont même ordre $2p$). Dans ce cas on a donc $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/2p\mathbb{Z}$ cyclique. Dans l'autre cas, G est non commutatif (puisque $tst^{-1} = s^{-1} \neq s$) ; il est engendré par s et t qui vérifient les relations $s^p = 1$, $t^2 = 1$ et $tst^{-1} = s^{-1}$. Dans ce cas G est isomorphe au groupe diédral $\mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ d'ordre $2p$.

Correction de l'exercice 5 ▲

(a) Le groupe G n'étant pas abélien n'est pas cyclique d'ordre 8 et possède au moins un élément $a \neq 1$ qui n'est pas d'ordre 2 (cf l'exercice **??**). Cet élément est nécessairement d'ordre 4. Le sous-groupe $H =< a >$ est distingué car d'indice 2.

(b) Supposons qu'il existe $b \in G \setminus H$ d'ordre 2 et posons $K =< b >$. On a $H \cap K = \{1\}$ car $b \notin H$. Le sous-groupe H étant distingué dans G, on peut écrire que $HK/H \simeq K$, ce qui donne $|HK| = |H|\,|K| = 8$ et donc $G = HK$. De plus, l'inclusion $K \subset G$ est une section de la suite exacte $1 \to H \to G \to K \to 1$. Le groupe G est donc isomorphe au produit semi-direct de H par K. L'action sur H du générateur b d'ordre 2 de K est nécessairement donnée par le passage à l'inverse (cf exercice 4).

(c) Dans le cas contraire à (b), tous les éléments de $G \setminus H$ sont nécessairement d'ordre 4. Les éléments de G d'ordre 2 sont donc dans H, qui n'en possède qu'un : a^2, qu'on note -1.

Le centre $Z(G)$ est d'ordre différent de 1 car G est un 2-groupe et différent de 8 car G est non abélien. Il n'est pas non plus d'ordre 4 car alors on aurait $G = Z(G) \cup xZ(G)$ pour un $x \in G \setminus Z(G)$ mais alors G serait abélien. Le centre $Z(G)$ est donc d'ordre 2. D'après ce qui précède $Z(G) = \{1, -1\}$.

Soit $b \in G \setminus H$. Alors G est engendré par a et b. D'autre part b est d'ordre 4 et b^2 d'ordre 2 ce qui entraine $b^2 = -1$. La conjugaison par b induit un automorphisme du sous-groupe distingué $< a >$; on a donc $bab^{-1} = a^{-1}$, le seul autre cas $bab^{-1} = a$ étant exclu car G non abélien. On obtient ensuite aisément que si $ab = c$, on a $c^2 = -1$ ($c^2 = abab = aa^{-1}bb = b^2 = -1$) et $ba = -ab = -c$, $bc = -cb = a$, $ca = -ac = b$.

Correction de l'exercice 7 ▲

(a) On a $\theta(g)(xH) = gxH$ $(g,x \in G)$. Le noyau de θ est l'intersection de tous les conjugués xHx^{-1} de H, c'est-à-dire, d'après les théorèmes de Sylow, l'intersection de tous les 3-Sylow de G. Comme l'intersection de deux 3-Sylow distincts est triviale, le noyau est $\neq \{1\}$ si et seulement s'il n'existe qu'un seul 3-Sylow, qui est alors automatiquement distingué dans G.

Si H est non distingué dans G, alors θ est injectif et fournit un isomorphisme entre G et un sous-groupe de S_4. Ce sous-groupe devant être d'ordre 12 comme G, c'est nécessairement A_4 (cf l'exercice **??**).

(b) Si G n'est pas isomorphe à A_4, alors nécessairement H est distingué dans G et c'est alors l'unique 3-Sylow de G. Notons $1, a, a^2$ les trois élément distincts du groupe cyclique H.

Supposons que G contienne un élément b d'ordre 4. On a $b^4 = a^3 = 1$. D'autre part, la conjugaison par b laissant invariant le sous-groupe distingué $H = <a>$, l'élément bab^{-1} doit être un générateur de $<a>$, c'est-à-dire a ou a^{-1}. Mais la première possibilité est exclue car sinon b serait dans le centre de G et G serait abélien (cf exercice **??**). La seconde possibilité existe bien : on prend par exemple pour G le produit semi direct $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ où l'action de $\mathbb{Z}/4\mathbb{Z}$ sur $\mathbb{Z}/3\mathbb{Z}$ se fait à travers la surjection canonique $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, c'est-à-dire, les classes de 0 et 2 modulo 4 agissent comme l'identité et celles de 1 et 3 comme le passage à l'inverse.

Supposons au contraire qu'aucun élément de $G \setminus H$ soit d'ordre 4. Les 2-Sylow sont donc isomorphes au groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. De plus, deux quelconques B et B' d'entre eux sont forcément d'intersection non triviale car sinon l'ensemble produit BB' (qui est en bijection avec $B \times B'$ par $(b,b') \to bb'$) serait de cardinal $|B|\,|B'| = 16 > 12$. Il y a donc strictement moins de $3 \times 3 = 9$ éléments d'ordre 2 dans G. Comme $G \setminus H$ est de cardinal 9, il existe dans G un élément c d'ordre $\neq 2$. Cet élément ne pouvant non plus être d'ordre 3 (H est le seul 3-Sylow), ni d'ordre 4 (par hypothèse) est d'ordre 6. Le groupe $<c>$ est alors d'indice 2 et donc distingué dans G. Comme $<c>$ est cyclique, il ne possède qu'un seul élément d'ordre 2. On peut donc trouver dans un 2-Sylow de G un élément $d \in G \setminus <c>$ d'ordre 2. La conjugaison par d induit un automorphisme de $<c>$ qui envoie c sur un générateur de $<c>$, c'est-à-dire ou bien c ou bien c^{-1}. Mais la première possibilité est exclue car G n'est pas abélien. On a donc $dcd^{-1} = c^{-1}$; le groupe G est dans ce cas isomorphe au groupe diédral D_6.

(c) Les groupes d'ordre 12 sont
- les groupes abéliens : $\mathbb{Z}/3Z \times \mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}/12\mathbb{Z}$ et $\mathbb{Z}/3 \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, et
- les groupes non abéliens : A_4, $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ (pour l'action donnée ci-dessus) et D_6.

Correction de l'exercice 9 ▲

Le groupe P est un p-sous groupe maximal de G et donc aussi de HP puisque $P \subset HP$ (noter que HP est un sous-groupe car H est supposé distingué dans G) ; P est donc un p-Sylow de HP. Si $|P| = p^n$, alors $|HP| = p^n s$ avec p ne divisant pas s. On peut aussi écrire $|H| = p^m r$ avec p ne divisant pas r ; on a alors nécessairement $m \leqslant n$ et s multiple de r. On a aussi $HP/H \simeq P/(H \cap P)$ ce qui donne $|H \cap P| = |P||H|/|HP| = p^m(r/s)$. On obtient donc que $s = r$ et que $H \cap P$ est un p-Sylow du groupe H.

On a aussi $|G| = p^n t$ avec p ne divisant pas t et t multiple de s. On en déduit $|G/H| = p^{n-m}(t/r)$. Comme t/r est un entier non divisible par p et que HP/H est un sous-groupe de G/H d'ordre $|HP/H| = p^{n-m}$, le groupe HP/H est un p-Sylow de G/H.

Correction de l'exercice 10 ▲

D'après les théorèmes de Sylow, le nombre de 5-Sylow d'un groupe d'ordre $200 = 5^2.2^3$ est $\equiv 1$ [mod 5] et divise 8. Ce ne peut être que 1. L'unique 5-Sylow est nécessairement distingué puisque ses conjugués sont des 5-Sylow et coincident donc avec lui. Le groupe ne peut pas être simple.

Correction de l'exercice 11 ▲

Les p-Sylow de S_p sont d'ordre p puisque p, étant premier, ne divise pas $p!/p = (p-1)!$. Chaque p-Sylow est donc cyclique d'ordre p et contient $p-1$ éléments d'ordre p. Les éléments d'ordre p de S_p sont les p-cycles ; il y en a $(p-1)!$. Il y a donc $(p-2)!$ p-Sylow. (On retrouve le théorème de Wilson : $(p-2)! \equiv 1$ [mod p] (ou $(p-1)!+1 \equiv 0$ [mod p]) si p est premier).

Correction de l'exercice 13 ▲

Le groupe alterné A_5 est d'ordre $60 = 2^2.3.5$.

Les 5-Sylow sont d'ordre 5, donc cycliques ; chacun est engendré par un 5-cycle et contient 4 5-cycles. Les 5-Sylow sont deux à deux d'intersection réduite à $\{1\}$. Comme il y a 24 5-cycles dans A_5, il y a 6 5-Sylow. (On peut aussi utiliser les théorèmes de Sylow : Le nombre de 5-Sylow est $\equiv 1$ [mod 5] et divise 12 ; c'est donc 1 ou 6. Comme ce ne peut être 1 (car il y aurait alors un unique 5-Sylow qui serait distingué, ce qui est impossible car A_5 est simple), c'est 6.)

Les 3-Sylow sont d'ordre 3, donc cycliques ; chacun est engendré par un 3-cycle et contient 2 3-cycles. Les 3-Sylow sont deux à deux d'intersection réduite à $\{1\}$. Comme il y a 20 3-cycles dans A_5, il y a 10 3-Sylow. (Par les théorèmes de Sylow : le nombre de 3-Sylow est $\equiv 1$ [mod 3] et divise 20 ; c'est donc 1, 4 ou 10. Comme ci-dessus, ce ne peut être 1. Si c'etait 4, la conjugaison de A_5 sur ces 3-Sylow induirait un morphisme $A_5 \to S_4$ non trivial (puisque cette action par conjugaison est transitive) et donc injectif (puisque le noyau, distingué, est forcément trivial). Or l'ordre de A_5 ne divise pas celui de S_4. Il y a donc 10 3-Sylow.)

Les 2-Sylow sont d'ordre 4, donc commutatifs. Comme il n'y a pas d'élément d'ordre 4 dans A_5, chaque 2-Sylow est isomorphe au groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; il est engendré par deux produits de deux transpositions qui commutent et contient 3 éléments d'ordre 2. On voit ensuite que ces trois éléments d'ordre 2 sont les 3 produits de deux transpositions qui commutent qu'on peut former avec quatre éléments de $\{1,\ldots,5\}$. On en déduit que les 2-Sylow sont deux à deux d'intersection réduite à $\{1\}$. Il y a 15 éléments d'ordre 2 dans A_5 et il y a 5 2-Sylow.

Tout élément de A_5 est d'ordre 1, 2, 3 ou 5 et est donc contenu dans un p-Sylow. On a bien $6.4+10.2+5.3+1 = 60$.

Correction de l'exercice 14 ▲

(a) Le nombre de 5-Sylow dans un groupe G d'ordre $60 = 2^2.3.5$ est $\equiv 1$ [mod 5] et divise 12. Comme G est supposé simple, ce ne peut être 1 ; il y a donc 6 5-Sylow. Le morphisme $\alpha : G \to S_6$ correspondant à l'action de G par conjugaison sur les 5-Sylow (une fois une numérotation des 5-Sylow de G choisie) est forcément injectif puisque son noyau, étant un sous-groupe distingué différent de G (d'après les théorèmes de Sylow, G agit transitivement sur les 5-Sylow), est nécessairement trivial. Considérons ensuite le groupe $\alpha^{-1}(A_6)$. C'est un sous-groupe distingué de G (comme image réciproque par un morphisme du sous-groupe distingué A_6 de S_6). Si $\alpha^{-1}(A_6) = \{1\}$ alors, pour tout $g \in G$, comme $\alpha(g^2) = \alpha(g)^2 \in A_6$, on aurait $g^2 = 1$ et donc G abélien, ce qui est absurde. On a donc $\alpha^{-1}(A_6) = G$, c'est-à-dire, $\alpha(G) = H \subset A_6$.

(b) Notons $\varphi : A_6 \to S_6$ le morphisme correspondant à l'action de A_6 par translation à gauche sur $A_6/.H$ (une fois une numérotation des éléments de $A_6/.H$ choisie). En utilisant la simplicité de A_6, on montre comme ci-dessus que φ est injectif et que $\varphi(A_6) \subset A_6$. Il en découle que φ est un isomorphisme entre A_6 et $\varphi(A_6) = A_6$.

(c) Un élément $x \in A_6$ fixe la classe neutre H si et seulement si $x \in H$. On obtient que H est isomorphe, *via* φ, au fixateur d'un entier, disons 6, dans l'action de A_6 sur $\{1,\ldots,6\}$, c'est-à-dire, à $A_6 \cap S_5 = A_5$.

Correction de l'exercice 17 ▲

Le nombre de q-Sylow d'un groupe G d'ordre p^2q est $\equiv 1$ [mod q] et divise p^2. Ce ne peut être ni p ni p^2 car p^2-1 est supposé non divisible par q ; c'est donc 1. De même le nombre de p-Sylow est $\equiv 1$ [mod p] et divise q et ce ne peut être q car $q-1$ est supposé non divisible par p ; c'est donc 1. Ainsi il y a un unique p-Sylow P d'ordre p^2, et donc abélien, et un unique q-Sylow Q d'ordre q, et donc cyclique, tous deux nécessairement distingués. Il en résulte que tout élément $x \in P$ commute avec tout élément $y \in Q$: en effet le commutateur $xyx^{-1}y^{-1} = (xyx^{-1})y^{-1} = x(yx^{-1}y^{-1})$ est dans l'intersection $P \cap Q$ qui est le groupe trivial. Cela montre que le groupe PQ est abélien ; il est isomorphe au produit direct $P \times Q$ et est donc de cardinal $|P|\,|Q| = p^2q = |G|$. D'où finalement $G = PQ$ est abélien.

Correction de l'exercice 18 ▲

Soit G un groupe d'ordre p^2q qu'on suppose simple. On distingue deux cas :

1er cas : $p > q$. Le nombre de p-Sylow de G est $\equiv 1$ [mod p] et divise q. Comme G est simple, ce ne peut être 1 (car sinon l'unique p-Sylow serait distingué). Il y a donc q p-Sylow d'ordre p^2, lesquels sont conjugués.

L'action par conjugaison de G sur ces q p-Sylow définit un morphisme $G \to S_q$ non trivial (car l'action est transitive) et donc injectif puisque le noyau, distingué et $\neq G$, est forcément trivial. On en déduit que p^2q divise $q!$ et donc p divise un entier entre 1 et $q-1$, ce qui contredit l'hypothèse $p > q$.

2ème cas : $p < q$. Le nombre de q-Sylow de G est $\equiv 1$ [mod q] et divise p^2. Comme ci-dessus, G étant simple, ce ne peut être 1. Ce ne peut-être ni p ni p^2. En effet, dans le cas contraire, p serait $\equiv \pm 1$ [mod q] et donc $p \geqslant q-1$. Comme $p < q$, la seule possibilité est $p = q-1$ et donc $p = 2$ et $q = 3$. Dans ce dernier cas, il y a 4 3-Sylow d'ordre 3 qui contiennent 8 éléments d'ordre 3. Ne reste de la place que pour un seul 2-Sylow qui devrait être distingué. Ce dernier cas n'est donc lui non plus pas possible.

Conclusion : il n'existe pas de groupe G simple d'ordre p^2q.

Correction de l'exercice 19 ▲

(a) Le nombre de 19-Sylow de G est $\equiv 1$ [mod 19] et divise 21 ; ce ne peut être que 1. Le groupe G a donc un unique 19-Sylow P qui est distingué.

(b) Comme P est distingué dans G, $N = PQ$ est un sous-groupe de G. De $P \cap Q = \{1\}$, on déduit que $PQ/P \simeq Q$ et donc que PQ est d'ordre $7.19 = 133$. D'après l'exercice 15, le groupe N est isomorphe au produit direct $\mathbb{Z}/19\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$, lequel est isomorphe au groupe cyclique $\mathbb{Z}/133\mathbb{Z}$ par le lemme chinois.

(c) Le nombre de 7-Sylow de G est $\equiv 1$ [mod 7] et divise 57. Les seules possibilités sont 1 et 57. Or ce n'est pas 1 non plus car on suppose que Q n'est pas distingué. Le groupe G admet donc 57 7-Sylow, et donc 57 sous-groupes cycliques d'ordre 133 par la question précédente. Ces 57 groupes d'ordre 133 sont bien distincts car deux 7-Sylow distincts engendrent avec P deux groupes cycliques d'ordre 133 distincts puisque le 7-Sylow est l'unique sous-groupe d'ordre 7 du groupe cyclique. Par conséquent leurs ensembles de générateurs sont deux à deux disjoints. On obtient ainsi $57 \times \phi(133) = 57 \times 6 \times 18$ éléments d'ordre 133 dans G (ϕ désigne ici la fonction indicatrice d'Euler), ce qui est manifestement absurde. On peut donc conclure que Q est distingué dans G et que l'unique sous-groupe cyclique $N = PQ$ d'ordre 133 l'est aussi.

(d) Comme N est distingué dans G, NR est un sous-groupe de G. De $N \cap R = \{1\}$, on déduit que $NR/N \simeq R$ et donc que NR est d'ordre $133.3 = 399$. Ainsi $G = NR$ et l'isomorphisme précédent $G/N \simeq R$ montre que l'inclusion $R \to G$ est une section de la suite exacte $1 \to N \to G \to R \to 1$. Le groupe G est donc isomorphe au produit semi-direct du groupe cyclique N d'ordre 133 par le groupe cyclique R d'ordre 3.
