Université Pierre & Marie Curie — Année 2008-2009
Master de Mathématiques — MM014 Théorie des groupes
Professeur: J.F. Dat — E. Brugallé

Feuille 1

Corrigé

Théorèmes d'isomorphisme

Solution 1

a)Soient $h \in H$ et $k \in K$. Alors $hk = kk^{-1}hk$ et comme H est distingué dans G, $k^{-1}hk \in H$ et donc $hk = kk^{-1}hk \in KH$. Donc $HK \subset KH$.
De même, avec la relation $kh = khk^{-1}k$, on a $KH \subset HK$ et donc $KH = HK$.
Pour tous $h, h' \in H$ et $k, k' \in K$, on a

$$hk(h'k')^{-1} = hkk'^{-1}h'^{-1} \in HKH = KHH = KH$$

donc HK est un sous groupe de G.
Puisque H est un sous groupe distingué de G, H est distingué dans HK.
Soient $g \in H \cap K$ et $k \in K$. Comme $g \in H$ et que H est distingué, on a $kgk^{-1} \in H$. Comme $g \in K$, on a aussi $kgk^{-1} \in H \cap K$. C'est à dire $H \cap K$ est distingué dans K.

b)On définit le morphisme de groupe suivant :

$$\begin{array}{rccc} \varphi & K & \longrightarrow & KH/H \\ & x & \longmapsto & \text{classe de } x \text{ dans } KH/H \end{array}$$

Comme K est un sous groupe de KH, cette application est bien définie. On maintenant montrer que φ est surjective et que son noyau est $H \cap K$.
On a $\varphi(x) = 1$ si et seulement si $x \in H$, donc $Ker(\varphi) = H \cap K$.
Soit $y \in KH/H$. Donc il existe $h \in H$ et $k \in K$ tels que $y = khH$. Mais alors $y = kH$, c'est à dire $y = \varphi(k)$, et φ est surjective.
Donc on a bien un isomorphisme $\varphi : K/(K \cap H) \to KH/H$.

Solution 2

a)Tout sous groupe de G est envoyé sur un sous groupe de G/H par π. On a donc bien une application induite

$$\widetilde{\pi} : \{A \text{ sous-groupe de } G \text{ contenant } H\} \to \{B \text{ sous-groupe de } G/H\}.$$

Comme $B = \widetilde{\pi}(\pi^{-1}(B))$, et que $H = \pi^{-1}(1) \subset \pi^{-1}(B)$, l'application $\widetilde{\pi}$ est surjective. Si $\pi(A) = \pi(A')$, cela équivaut à $A = HA'$. Donc si $H \subset A'$, on a $A = A'$ et $\widetilde{\pi}$ est injective.
Donc $\widetilde{\pi}$ est une bijection, et tout sous groupe de G/H peut s'écrire de manière unique A/H avec A un sous groupe de G contenant H.

b) A est distingué dans G si et seulement si $gAg^{-1} = A$ pour tout $g \in G$, donc si et seulement si $(gAg^{-1})/H = A/H$. Comme $(gAg^{-1})/H = g(A/H)g^{-1}$, A est distingué dans G si et seulement si A/H est distingué dans G/H.

c)Donc si A est distingué dans G, on a le morphisme de groupe suivant :

$$\begin{array}{cccc} \varphi & G & \longrightarrow & (G/H)/(A/H) \\ & x & \longmapsto & \text{classe de } x \text{ dans } (G/H)/(A/H) \end{array}$$

Etant la composée de deux surjection, φ est une surjection. Si $\varphi(x) = 1$, cela veut dire que $\pi(x) \in A/H$, et que donc $x \in A$. Donc $ker\varphi = A$ et on a un isomorphisme $\varphi : G/A \to (G/H)/(A/H)$.

Solution 3

1. *Il faut montrer que φ envoie deux éléments conjugués sur deux éléments conjugués. Comme φ est un morphisme de groupes, on a $\varphi(hgh^{-1}) = \varphi(h)\varphi(g)\varphi(h)^{-1}$ et donc $\varphi(hgh^{-1})$ et $\varphi(g)$ sont bien conjugués.*
2. *Soit $g \in Ker\ \varphi$. Alors la classe de conjugaison de g est envoyée sur la classe de conjugaison de $1_{G'}$. Mais 1_G est déjà envoyé sur la classe de conjugaison de $1_{G'}$, donc comme $\widetilde{\varphi}$ est injective, $g = 1_G$.*
3. *Soit $h \in G'$. Par surjectivité de $\widetilde{\varphi}$, h est conjugué dans G' à un élément de la forme $\varphi(g)$, c'est à dire qu'il existe $k \in G'$, $h = k\varphi(g)k^{-1}$.*
4. *Si il existe $g \in G$ tel que $h = k\varphi(g)^{-1}$, alors il est évident que $h\varphi(G)h^{-1} = k\varphi(g^{-1}Gg)k^{-1} = k\varphi(G)k^{-1}$.*
5. *On a donc $G' = \cup_{k \in G'/\varphi(G)} k\varphi(G)k^{-1}$ et donc $|G'| \leq \sum_{k \in G'/\varphi(G)} |\varphi(G)| = |G'/\varphi(G)||\varphi(G)| = |G'|$ et l'égalité a lieu si et seulement si les classes $(k\varphi(G)k^{-1})_{k \in G'/\varphi(G)}$ forment une partition de G'. Mais elle ont toutes l'élément neutre en commun, donc $|G'/\varphi(G)| = 1$, c'est à dire $G' = \varphi(G)$.*

Groupes cycliques

Solution 4

a) Soit $d = (k, n)$ le pgcd de k et de n. Les représentants modulo m des éléments du sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par la classe de k modulo n sont de la forme $ku + nv$, avec u et v dans $\mathbb{Z}$. Ce sont donc les multiples de $d = (k, n)$. Leurs classes modulo n sont au nombre de n/d.

Un morphisme de $\mathbb{Z}/m\mathbb{Z}$ dans un groupe G est entièrement déterminé par l'image de (la classe de) 1. Cette image est un élément g de G qui doit satisfaire la seule condition $g^m = 1$ (ou $mg = 0$ si la notation est additive). Dans $\mathbb{Z}/n\mathbb{Z}$, il y a exactement (m, n) tels éléments, le nombre cherché est donc (m, n).

b) Un élément d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ est un générateur de l'unique sous-groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$. Ce sous-groupe étant lui-même cyclique, c'est à dire isomorphe à $\mathbb{Z}/d\mathbb{Z}$, il a $\varphi(d)$ générateurs, ou φ est la fonction indicatrice d'Euler définie dans le cours.
On regroupe les n éléments du groupe $\mathbb{Z}/n\mathbb{Z}$ en classes formées des éléments de même ordre, et on obtient la formule désirée.

c) Si $\psi(d)$ n'est pas nul, il y a un élément de G qui est d'ordre d. Le groupe H que cet élément engendre a d éléments, lesquels sont tous racines du polynôme $X^d - 1$. On en déduit que ce polynôme n'a pas d'autre racine, et que tous les éléments d'ordre d de G sont des générateurs du groupe cyclique H. Il y en a donc $\varphi(d)$.

d) On regroupe les n éléments du groupe G en classes formées des éléments de même ordre, comme dans la question b).

e) En faisant la différence des équations des questions a) et b), on trouve $\sum_{d|n}(\varphi(d) - \psi(d)) = 0$. Mais on a vu au c) que chacun des termes de cette somme est positif ou nul. On en déduit qu'il sont tous nuls. En particulier, $\psi(n) = \varphi(n) > 0$, et G admet au moins un élément d'ordre n, c'est-à-dire que G est cyclique.

Solution 5

a) On a bien sûr $(xy)^{mn} = x^{mn}y^{mn} = (x^m)^n(y^n)^m = 1$, donc l'ordre de xy est un diviseur de mn. D'autre part, si $k \geq 1$ est tel que $(xy)^k = 1$, on a $1 = (xy)^{km} = x^{km}y^{km} = y^{km}$ On en déduit que km est un multiple de n, donc k est un multiple de n puisque m et n sont premiers entre eux. De même, k est un multiple de m et donc de mn, qui est bien l'ordre de xy.

b) On peut prendre $m' = \prod_{v_p(m) \geq v_p(n)} p^{v_p(m)}$ et $n' = \prod_{v_p(m) < v_p(n)} p^{v_p(n)}$, le produit étant pris sur les nombres premiers qui divisent mn.

c) Il suffit de constater que $x^{m/m'}$ est d'ordre m' et $y^{n/n'}$ est d'ordre n'. D'après la question a), $x^{m/m'}y^{n/n'}$ est d'ordre $m'n' = \mathrm{ppcm}(m, n)$.

d) Comme l'ordre des éléments de G est borné, il existe un élément x d'ordre maximal, disons m. Si m est un diviseur strict de N, il existe un élément y de G tel que $y^m \neq 1$. Si n est l'ordre de y, on a montré à la question précédente qu'il existait dans G un élément d'ordre $\mathrm{ppcm}(m, n) > m$, une contradiction. L'exposant du groupe $\mathcal{S}_3$ est 6, et il n'y a pas d'élément d'ordre 6 dans $\mathcal{S}_3$.

e) Si G est un sous-groupe fini du groupe multiplicatif d'un corps, il a un exposant N et un élément x d'ordre N. Le groupe H engendré par x est d'ordre N et tous ses éléments sont racines du polynôme $X^N - 1$. Ce polynôme n'a donc pas d'autre racine. Comme tous les éléments de G en sont racines, $G \subset H$ et G est cyclique.

Restes chinois

Solution 6 *De façon générale, les congruences $k \equiv a \pmod{m}$ et $k \equiv b \pmod{n}$ ont une solution commune si et seulement si on a $a \equiv b \pmod{d = (m,n)}$. La solution est alors unique modulo le ppcm mn/d de m et n.*

a) $k \equiv 33 \pmod{35}$,

b) $k \equiv 22 \pmod{30}$,

c) Pas de solution.

Solution 7

a) L'application qui à f fait correspondre $f(1)$ est une bijection de l'ensemble des endomorphismes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$. La bijection réciproque fait correspondre à k l'endomorphisme f_k défini par $f_k(x) = kx$. On voit que l'on a $f_k + f_l = f_{k+l}$ et $f_k \circ f_l = f_{kl}$, ce qui fait que la bijection en question est un isomorphisme d'anneaux entre $\mathrm{End}(\mathbb{Z}/n\mathbb{Z})$ et $\mathbb{Z}/n\mathbb{Z}$. Le groupe $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ des automorphismes de $(\mathbb{Z}/n\mathbb{Z})$ est le groupe des éléments inversibles de $\mathrm{End}(\mathbb{Z}/n\mathbb{Z})$. Il correspond donc au groupe $(\mathbb{Z}/n\mathbb{Z})^*$ des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

b) C'est une conséquence directe du théorème des restes chinois. L'application naturelle de $\mathbb{Z}/n\mathbb{Z}$ dans $\prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ est un isomorphisme d'anneaux : les groupes des éléments inversibles de chaque côté sont donc isomorphes.

c) On a vu dans les exercices 1 et 2 que tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique. C'est donc le cas de $(\mathbb{Z}/p\mathbb{Z})^*$, qui a donc un élément d'ordre $p-1$. Si a est un représentant dans $\mathbb{Z}$ d'un tel élément, l'ordre de la classe de a dans $\mathbb{Z}/p^\alpha\mathbb{Z}$ est un multiple de $p-1$ et un diviseur de $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$. En prenant au besoin a^{p^k} pour un $k > 0$ plutôt que a, on obtient un élément b de $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ qui est d'ordre exactement $p-1$.
D'autre part, le développement de

$$(1+x)^p = 1 + px + \binom{p}{2}x^2 + \ldots \binom{p}{p-1}x^{p-1} + x^p$$

permet de montrer que si $x = 0 \ mod \ p^k$, alors $(1+x)^p = 1 \ mod \ p^{k+1}$. On en déduit par récurrence que $(1+p)^{p^{\alpha-2}} \neq 1 \ mod \ p^\alpha$ et $(1+p)^{p^{\alpha-1}} = 1 \ mod \ p^\alpha$. Donc l'ordre de $1+p$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ est $p^{\alpha-1}$. L'élément $b(1+p)$ est donc un générateur de $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$.

d) On a $(\mathbb{Z}/2\mathbb{Z})^* = \{1\}$, $(\mathbb{Z}/4\mathbb{Z})^* = \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}$ *et* $(\mathbb{Z}/8\mathbb{Z})^* = \{\pm 1, \pm 5\} \simeq (\mathbb{Z}/2\mathbb{Z})^2$. *Comme à la question précédente, le développement* $(1+x)^2 = 1 + 2x + x^2$ *montre que si* $v_2(x) = k \geq 2$ *alors* $(1+x)^2 = 1 + y$, *avec* $v_2(y) = k+1$. *Par récurrence, la valuation 2-adique de* 5^{2^α} *est donc* $\alpha + 2$ *et l'ordre de* 5 *dans* $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ *est* $2^{\alpha-2}$. *Le sous-groupe engendré par 5 est en somme directe avec le sous-groupe* $\{\pm 1\}$, *d'où le résultat.*

e) le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *a trois éléments non nuls d'ordre 2, et la somme de deux éléments non nuls égale le troisième. On en déduit que toute permutation de ces trois éléments donne un automorphisme de* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. *Le groupe* $Aut(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ *est donc naturellement isomorphe au groupe symétrique* $\mathcal{S}_3$ *sur trois éléments, le plus petit groupe non commutatif.*

Solution 8

1. $(\mathbb{Z}/11\mathbb{Z})^*$ *est le groupe multiplicatif des éléments non nuls du corps* $\mathbb{F}_{11}$, *donc est cyclique d'ordre 10,* $(\mathbb{Z}/10\mathbb{Z})^* \simeq (\mathbb{Z}/5\mathbb{Z})^* \times (\mathbb{Z}/2\mathbb{Z})^* \simeq \mathbb{F}_5^*$ *est cyclique d'ordre 4,* $(\mathbb{Z}/9\mathbb{Z})^*$ *est d'ordre* $3\varphi(3) = 6$, *et cyclique, car* $x = \overline{2}$ *vérifie* $x^2 \neq 1, x^3 \neq 1$, *donc est d'ordre 6 . En revanche,* $(\mathbb{Z}/2^\alpha\mathbb{Z})^* \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{\alpha-2}\mathbb{Z})$ *est d'ordre* $2^{\alpha-1}$, *non cyclique.*
2. $N = 2^4.32.5.11$, *donc* $\mathbb{Z}/N\mathbb{Z} \simeq (\mathbb{Z}/16\mathbb{Z}) \times (\mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z})$ *et* $(\mathbb{Z}/N\mathbb{Z})^* \simeq (\mathbb{Z}/16\mathbb{Z})^* \times (\mathbb{Z}/9\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^* \times (\mathbb{Z}/11\mathbb{Z})^* \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/10\mathbb{Z})$. *L'exposant est le ppcm des ordres des éléments du groupe, donc vaut 60.*
3. *Les éléments d'ordre divisant* 5 *de* $(\mathbb{Z}/N\mathbb{Z})^*$ *sont en bijection avec les solutions dans* $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/10\mathbb{Z})$ *de l'équation* $5(x_2, x_4, x_6, x_4', x_{10}) = 0$, *i.e.* $x_2 = ... = x_4' = 0, x_{10} = \{0, 2, 4, 6, 8\}$. *Il a donc 5 solutions.*

Groupe symétrique

Solution 9

	Id	$(1,2)$	$(2,3)$	$(1,3)$	$(1,2,3)$	$(1,3,2)$
Id	Id	$(1,2)$	$(2,3)$	$(1,3)$	$(1,2,3)$	$(1,3,2)$
$(1,2)$	$(1,2)$	Id	$(1,2,3)$	$(1,3,2)$	$(2,3)$	$(1,3)$
$(2,3)$	$(2,3)$	$(1,3,2)$	Id	$(1,2,3)$	$(1,3)$	$(1,2)$
$(1,3)$	$(1,3)$	$(1,2,3)$	$(1,3,2)$	Id	$(1,2)$	$(2,3)$
$(1,2,3)$	$(1,2,3)$	$(1,3)$	$(1,2)$	$(2,3)$	$(1,3,2)$	Id
$(1,3,2)$	$(1,3,2)$	$(2,3)$	$(1,3)$	$(1,2)$	Id	$(1,2,3)$

Le groupe $\mathcal{S}_3$ *a 6 sous-groupes :* $\{Id\}$, $\mathcal{A}_3 = \{Id, (1,2,3), (1,3,2)\}$ *et* $\mathcal{S}_3$ *sont distingués,* $\{Id, (1,2)\}$, $\{Id, (1,3)\}$ *et* $\{Id, (2,3)\}$ *ne le sont pas.*
Le groupe $\mathcal{A}_4$ *a 10 sous-groupes :* $\{Id\}$,

$$\{Id, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

et $\mathcal{A}_4$ sont distingués, $\{Id, (1,2)(3,4)\}$, $\{Id, (1,3)(2,4)\}$, $\{Id, (1,4)(2,3)\}$, ainsi que $\{Id, (1,2,3), (1,3,2)\}$, $\{Id, (1,2,4), (1,4,2)\}$, $\{Id, (1,3,4), (1,4,3)\}$ et $\{Id, (2,3,4), (2,4,3)\}$ ne le sont pas.

Solution 10

a) On a $(x_1, x_2, \ldots, x_{k-1}, x_k) = (1, x_1)(1, x_k)(1, x_{k-1}) \ldots (1, x_2)(1, x_1)$ si 1 ne fait pas partie des x_i et $(1, x_2, \ldots, x_{k-1}, x_k) = (1, x_k)(1, x_{k-1}) \ldots (1, x_2)$, donc les transpositions données engendrent tous les cycles, et $\mathcal{S}_n$ tout entier. Si on oublie la transposition $(1, i)$, on ne peut obtenir que des permutations qui laissent i fixe, donc pas $\mathcal{S}_n$ tout entier.

b) On a $(1, i) = (1, 2)(2, 3) \ldots (i-2, i-1)(i-1, i)(i-2, i-1) \ldots (2, 3)(1, 2)$ donc les $(1, i)$ sont dans le groupe engendré. Or on a vu à la question précédente que les $(1, i)$ engendraient $\mathcal{S}_n$. Donc les $(i, i+1)$ engendrent $\mathcal{S}_n$. Si on omet la transposition $(i, i+1)$, toute permutation du groupe engendré laisse stable l'ensemble $\{1 \ldots i\}$, ce ne peut donc être $\mathcal{S}_n$ entier.

c) Si on pose $\sigma = (1, 2, \ldots, n)$ et $\tau = (1, 2)$, on a $(i, i+1) = \sigma^{i-1}\tau\sigma^{1-i}$. D'après la question précédente, le groupe engendré est $\mathcal{S}_n$. La minimalité est ici évidente.

d) Si la transposition est (i, j), posons $a = j - i$. On a

$$\sigma^{1-i}(i, j)\sigma^{i-1} = (1, j - i + 1) = (1, a + 1) = \tau,$$

puis

$$\sigma^{ka}\tau\sigma^{-ka} = (ka + 1, (k + 1)a + 1) = \tau_k$$

et

$$(1, ka + 1) = \tau\tau_1\tau_2 \ldots \tau_{k-2}\tau_{k-1}\tau_{k-2} \ldots \tau_2\tau_1\tau$$

pour tout $k \geq 1$ (les entiers sont à comprendre modulo n). Comme n est premier et a non nul modulo n, il existe un entier $k \geq 1$ tel que $ka \equiv 1 \pmod{n}$. On a donc montré que $(1, 2)$ appartient au groupe engendré, qui est donc $\mathcal{S}_n$ d'après la question précédente.

Solution 11

a) Pour toute permutation (paire) différente de Id, notons $m(\sigma)$ le plus grand entier m tel que $\sigma(m) = k \neq m$. Montrons par récurrence sur $m(\sigma)$ que σ s'écrit comme produit de $\sigma_i = (1, 2, i)$. Si $m(\sigma) \leq 2$, comme σ est paire, σ est en fait Id. Supposons donc $m = m(\sigma) > 2$. On considère $\tau = (1, m, 2)(1, 2, k)\sigma$ si $k = \sigma(m) > 2$, $\tau = (1, 2, m)\sigma$ si $k = 2$ et $\tau = (1, m, 2)\sigma$ si $k = 1$. Dans tous les cas, on a $\tau(m) = m$ et $m(\tau) < m(\sigma)$. D'après l'hypothèse de récurrence, τ appartient au groupe engendré par les σ_i. Il en est donc de même de σ.

b) On a $(1,2,4) = (1,2,3)(2,4,3)$*, puis*

$$(1,2,i+2) = (i,i+2,i+1)(1,2,i)(i,i+1,i+2)$$

pour $i \geq 3$*, donc les* $(1,2,i)$ *appartiennent au groupe engendré, ainsi que* $\mathcal{A}_n$ *d'après la question précédente.*

c) Si on oublie le 3-cycle $(1,2,i)$*, on ne peut obtenir que des permutations qui laissent* i *fixe, donc pas* $\mathcal{A}_n$ *tout entier. Par contre, la relation*

$$(2,3,4) = (3,4,5)(1,3,2)(3,5,4)(1,2,3)$$

montre que l'on peut omettre $(2,3,4)$ *du second système générateur.*

Solution 12 *On rappelle que si* $(a_1,\ldots,a_k)$ *est un* k*-cycle de* $\mathcal{S}_n$*, alors on a* $\sigma(a_1,\ldots,a_k)\sigma^{-1} = (\sigma(a_1),\ldots,\sigma(a_k))$ *pour tout* $\sigma \in \mathcal{S}_n$*.*

a)Soient (a,b,c) *et* (d,e,f) *deux 3-cycles dans* $\mathcal{A}_n$*, et soit* $\sigma \in \mathcal{S}_n$ *défini par* $\sigma(a) = d$*,* $\sigma(b) = e$ *et* $\sigma(c) = f$*. On a alors* $\sigma(a,b,c)\sigma^{-1} = (d,e,f)$*. Si* $\sigma \in \mathcal{A}_n$*, alors on a gagné. Sinon, on prend* $\sigma' = (d,e)\sigma \in \mathcal{A}_n$ *et on a alors* $\sigma'(a,b,c)\sigma'^{-1} = (e,d,f)$ *ou encore* $\sigma'(b,a,c)\sigma'^{-1} = (d,e,f)$*. Donc si un sous groupe distingué* G *de* $\mathcal{A}_n$ *contient un 3-cycle, il les contient tous. Comme les 3-cycles engendrent* $\mathcal{A}_n$*, on a* $G = \mathcal{A}_n$*.*

b)

- *Si* σ *a un cycle de longueur au moins 4 dans sa décomposition en cycles à supports disjoints. Soit* $(a,b,c,d,\ldots)$ *un tel cycle. Alors on a*

  $$(a,b,c,d,\ldots)(a,b,c)^{-1}(a,b,c,d,\ldots)^{-1} = (c,b,d)$$

  et

  $$(a,b,c)(a,b,c,d,\ldots)(a,b,c)^{-1}(a,b,c,d,\ldots)^{-1} = (a,b,d).$$

- *Si* σ *contient* $\sigma' = (a,b,c)(d,e)$ *dans sa décomposition en cycles à supports disjoints, alors*

  $$\sigma'(a,d)(b,e)\sigma'^{-1} = (b,e)(c,d)$$

  et

  $$(a,d)(b,e)\sigma'(a,d)(b,e\sigma'^{-1} = (a,d,c).$$

- *Si* σ *contient* $\sigma' = (a,b)(c)$ *dans sa décomposition en cycles à supports disjoints, alors*

  $$\sigma'(a,b,c)^{-1}\sigma'^{-1} = (a,b,c)$$

  et

  $$(a,b,c)\sigma'(a,b,c)^{-1}\sigma'^{-1} = (b,a,c).$$

- *Sinon, on se trouve dans un des autres cas énuméré dans la question.*

c)Soit G un sous groupe distingué de $\mathcal{A}_n$ non trivial. Alors il existe un élément $\sigma \neq 1 \in \mathcal{A}_n$. D'après la question a), il suffit de montrer que G contient un 3-cycle pour montrer que $G = \mathcal{A}_n$. D'après la question b), si σ n'est pas le produit de $n/2$ transpositions disjointes, ou le produit de 3-cycles et de 1-cycles disjoints, on a gagné.

- *Si σ n'est pas un 3-cycle et est le produit de 3-cycles et de 1-cycles, alors $n \geq 5$ et on a au moins deux 3-cyles. Si on pose $\sigma' = (a, b, c)(d, e, f)$ et $\tau = (a, b, d)$, on voit que*

$$\tau\sigma'\tau^{-1}\sigma'^{-1} = (a, b, e, c, d)$$

  et on s'est ramené à la question b).
- *Si σ est le produit de $n/2$ transpositions disjointes, comme $n \geq 5$, on en a au moins 3. Si on pose $\sigma' = (a, b)(c, d)(e, f)$ et $\tau = (a, c)(b, e)$, on voit que*

$$\tau\sigma'\tau^{-1}\sigma'^{-1} = (a, f, c)(b, d, e)$$

  et on s'est ramené au cas précédent.

En conclusion, $\mathcal{A}_n$ est simple pour $n \geq 5$. Il est facile de voir que c'est encore le cas pour $n \leq 3$ puisque $\mathcal{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$ et $\mathcal{A}_2 \simeq \mathcal{A}_1 \simeq \{Id\}$. Par contre, pour $n = 4$, on a vu que $\{Id, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$ était le seul sous-groupe distingué non trivial de $\mathcal{A}_4$.

Solution 13

a) On a vu que si $\sigma = (x_1, \ldots, x_n)$ est un n-cycle et τ une permutation, $\tau\sigma\tau^{-1} = (\tau(x_1), \ldots, \tau(x_n))$ est aussi un n-cycle. Dire que σ et τ commute, c'est dire que ce cycle est en fait σ. Ceci signifie que les éléments $(\tau(x_1), \ldots, \tau(x_n))$ sont les éléments $(x_1, \ldots, x_n)$ pris dans le même ordre, mais peut-être non pas à partir de l'élément numéro 1, mais à partir du numéro k, c'est-à-dire que $\tau = \sigma^k$.

b) Dans le cas général, écrivons sur une ligne les cycles de σ, y compris les k_1 qui sont de longueur 1. Pour que $\tau\sigma\tau^{-1} = \sigma$ il faut que τ permute les supports des cycles de σ. Comme on ne peut permuter que les cycles de même longueur, il y a $k_i!$ choix possibles pour les cycles de longueur i. Une fois la correspondance entre les cycles choisie, il y a i choix possible pour chaque cycle de longueur i, donc i^{k_i} choix pour l'ensemble des cycles de longueur i. La formule en découle.