THÉORIE DES GROUPES - SÉRIE 14

20 décembre 2019

Groupes quotients

Exercice 1. Soient $H_1, \ldots, H_n$ des sous-groupes normaux d'un groupe G. On considère l'application

$$\phi\colon G \to G/H_1 \times \ldots G/H_n,\ g \mapsto (gH_1, \ldots, gH_n).$$

(a) Montrer que $\mathrm{Ker}(\phi) = H_1 \cap \ldots \cap H_n$.

(b) Montrer que, si H_i est d'indice fini dans G, pour tout $1 \leq i \leq n$, et $([G : H_i], [G : H_j]) = 1$ pour tout $i \neq j \in \{1, \ldots, n\}$, alors ϕ est surjective et

$$[G : H_1 \cap \ldots \cap H_n] = \prod_{i=1}^{n} [G : H_i].$$

Solution.

(a) Soit $g \in G$ tel que $\phi(g) = e_{G/H_1 \times \ldots \times G/H_n}$. Alors $gH_i = H_i$ pour tout $1 \leq i \leq n$ et donc $g \in H_1 \cap \ldots \cap H_n$. Inversément, si $g \in H_1 \cap \ldots \cap H_n$, alors

$$\phi(g) = (gH_1, \ldots, gH_n) = (H_1, \ldots, H_n) = e_{G/H_1 \times \ldots \times G/H_n}.$$

Donc on a bien $\mathrm{Ker}(\phi) = H_1 \cap \ldots \cap H_n$.

(b) On note $m_i = [G : H_i]$. On a que, pour tout $1 \leq i \leq n$,

$$[G : H_1 \cap \ldots \cap H_n] = [G : H_i][H_i : H_1 \cap \ldots \cap H_n] = m_i[H_i : H_1 \cap \ldots \cap H_n].$$

Donc m_i divise $[G : H_1 \cap \ldots \cap H_n]$ pour tout $1 \leq i \leq n$. Comme les m_i sont premiers entre eux, $m_1 \cdots m_n$ divise $[G : H_1 \cap \ldots \cap H_n]$ et donc $[G : H_1 \cap \ldots \cap H_n] \geq m_1 \cdots m_n$. De plus, par le premier théorème d'isomorphisme et le point (a), $\mathrm{Im}(\phi) \cong G/(H_1 \cap \ldots \cap H_n)$, d'où

$$m_1 \cdots m_n = |G/H_1 \times \ldots \times G/H_n| \geq |\mathrm{Im}(\phi)| = [G : H_1 \cap \ldots \cap H_n].$$

Ainsi on obtient que $[G : H_1 \cap \ldots \cap H_n] = m_1 \cdots m_n = [G : H_1] \cdots [G : H_n]$ et que $\mathrm{Im}(\phi) = G/H_1 \times \ldots \times G/H_n$.

Groupes résolubles

Exercice 2. Soient G un groupe, $H < G$ un sous-groupe et $N < G$ un sous-groupe normal tels que H et N sont résolubles. Montrer que HN est résoluble.

Solution. Par le deuxième théorème d'isomorphisme, on a que $HN/N \cong H/(H \cap N)$. Le groupe $H/(H \cap N)$ est résoluble comme quotient du groupe résoluble H. Donc HN/N est aussi résoluble. Par un résultat du cours, comme HN/N et N sont résolubles, alors HN est aussi résoluble.

Actions de groupes

Exercice 3. Soient G un groupe qui agit sur un ensemble X et H un sous-groupe de G. Montrer que H agit transitivement sur X si et seulement si G agit transitivement sur X et $G = HG_x$, où $x \in X$.

Solution. Supposons d'abord que $H < G$ soit un sous-groupe qui agit transitivement sur X. Alors, pour $x \in X$,

$$X \supset \mathcal{O}_x = \{g \cdot x \mid g \in G\} \supset \{h \cdot x \mid h \in H\} = X.$$

Donc $\mathcal{O}_x = X$ et G agit transitivement sur X. Soit encore $g \in G$ et $x \in X$. Comme H agit transitivement sur X, il existe $h \in H$ tel que $h \cdot x = g \cdot x$. Alors $x = h^{-1}g \cdot x$ et donc $h^{-1}g \in G_x$. Ainsi $g = h(h^{-1}g) \in HG_x$ et on a bien $G = HG_x$.

Inversément, supposons que G agisse transitivement sur X et que $G = HG_x$ pour un certain $x \in X$. Soit $y \in X$. Par transitivité de l'action de G sur X, il existe $g \in G$ tel que $g \cdot x = y$. Comme $G = HG_x$, il existe $h \in H$ et $k \in G_x$ tels que $g = hk$. Ainsi $y = g \cdot x = hk \cdot x = h \cdot x$ et donc H agit transitivement sur X.

Exercice 4. Soit p un nombre premier.

(a) Soit G un p-groupe fini qui agit sur un ensemble fini X. Montrer que

$$|X| \equiv |X^G| \pmod{p}.$$

En déduire que si p ne divise pas $|X|$, alors l'action de G sur X admet des points fixes.

(b) Utiliser le point (a) pour montrer le **Petit Théorème de Fermat**:
Si $n \in \mathbb{N}$, alors $n^p \equiv n \pmod{p}$.

Solution.

(a) Remarquer d'abord que $x \in X^G$ si et seulement si $1 = |\mathcal{O}_x| = [G : G_x]$. Comme X est l'union disjointe des orbites de l'action de G, alors

$$|X| = \sum_{x \in R} |\mathcal{O}_x| = \sum_{x \in R} [G : G_x] = |X^G| + \sum_{x \in R \setminus X^G},$$

où $R \subset X$ est un ensemble de représentants des orbites de l'action de G sur X. Pour $x \in R \setminus X^G$, $[G : G_x]$ divise $|G| = p^k$, pour un certain $k \in \mathbb{N}$, et ne vaut pas 1. Donc, pour tout $x \in R \setminus X^G$, p divise $[G : G_x]$. Ainsi

$$|X| \equiv |X^G| \pmod{p}.$$

De plus, si p ne divise pas $|X|$, alors $|X^G| \not\equiv 0 \pmod{p}$ et donc X^G n'est pas vide.

(b) Soit Y un ensemble tel que $|Y| = n$. On pose $X = \prod_{i=1}^{p} Y$. Alors $\mathbb{Z}/p\mathbb{Z}$ agit sur X en permutant cycliquement les facteurs. L'ensemble des points fixes de cette action est

$$X^{\mathbb{Z}/p\mathbb{Z}} = \{(y_i)_{i=1}^n \mid y_1 = y_i \text{ pour tout } 1 \leq i \leq n\} = \{(y, \ldots, y) \mid y \in Y\}$$

et $|X^{\mathbb{Z}/p\mathbb{Z}}| = |Y| = n$. Comme $|X| = |Y|^p = n^p$, on conclut par le point (a) que

$$n^p \equiv n \pmod{p}.$$

Exercice 5. Soit $\phi\colon G \to G'$ un homomorphisme de groupes.

(a) Soient Y, Y' des G'-ensembles. Montrer que, si $v\colon Y \to Y'$ est une application G'-équivariante, alors $v\colon Y \to Y'$ est aussi G-équivariante, où Y et Y' sont des G-ensembles via l'action induite par ϕ, i.e. $g * y = \phi(g) \cdot y$ et $g * y' = \phi(g) \cdot y'$ respectivement, pour tout $g \in G$, $y \in Y$ et $y' \in Y'$. On note ${}^{\phi}v\colon {}^{\phi}Y \to {}^{\phi}Y'$ cette application G-équivariante.

(b) Soient X, X' des G-ensembles. Montrer qu'une application G-équivariante $u\colon X \to X'$ induit une application G'-équivariante

$$\overline{u} = G' \times_{\phi} u\colon G' \times_{\phi} X \to G' \times_{\phi} X',\ (g', x) \mapsto (g', u(x)).$$

Montrer également que:

(i) si $u = \mathrm{id}_X\colon X \to X$, alors $\overline{u} = \mathrm{id}_{G' \times_{\phi} X}$, et

(ii) si $u\colon X \to X'$ et $u'\colon X' \to X''$, alors $\overline{u' \circ u} = \overline{u'} \circ \overline{u}$.

(c) Définir

(i) pour tout G-ensemble X, une application G-équivariante $\eta_X\colon X \to {}^{\phi}(G' \times_{\phi} X)$, et

(ii) pour tout G'-ensemble Y, une application G'-équivariante $\epsilon_Y\colon (G' \times_{\phi} {}^{\phi}Y) \to Y$,

telles que les applications Φ et Ψ définie par

$$\Phi\colon \mathcal{F}_G(X, {}^{\phi}Y) \to \mathcal{F}_{G'}(G' \times_{\phi} X, Y),\ u \mapsto \epsilon_Y \circ \overline{u}$$

$$\Psi\colon \mathcal{F}_{G'}(G' \times_{\phi} X, Y) \to \mathcal{F}_G(X, {}^{\phi}Y),\ v \mapsto {}^{\phi}v \circ \eta_X$$

sont des inverses l'un de l'autre.

Remarque: Cette construction redonne la bijection $\mathcal{F}_G(X, {}^{\phi}Y) \cong \mathcal{F}_{G'}(G' \times_{\phi} X, Y)$ vue en cours.

Solution.

(a) Pour $g \in G$ et $y \in Y$, comme v est G'-équivariante, on a que

$$v(g * y) = v(\phi(g) \cdot y) = \phi(g) \cdot v(y) = g * v(y).$$

Donc v est bien G-équivariante pour les actions induites par ϕ.

(b) On vérifie d'abord que $\overline{u}$ est bien définie. Soient $g \in G$, $g' \in G'$ et $x \in X$. Alors

$$\overline{u}(g'\phi(g), x) = (g'\phi(g), u(x)) = (g', \phi(g) \cdot u(x)) = \overline{u}(g', g \cdot x).$$

Donc $(g'\phi(g), x) \sim (g', g \cdot x)$ sont bien envoyés sur la même image et $\overline{u}$ est bien définie. Si $u = \mathrm{id}_X$, alors

$$\overline{u}(g', x) = (g', u(x)) = (g', x)$$

et on a bien $\overline{u} = \mathrm{id}_{G' \times_{\phi} X}$. Finalement, si $u\colon X \to X'$ et $u'\colon X' \to X''$, alors

$$\overline{u'} \circ \overline{u}(g', x) = \overline{u'}(g', u(x)) = (g', u'(u(x))) = \overline{u' \circ u}(g', x)$$

et on a bien $\overline{u' \circ u} = \overline{u'} \circ \overline{u}$.

(c) On définit:

(i) pour un G-ensemble X, l'application η_X par

$$\eta_X \colon X \to {}^{\phi}(G' \times_{\phi} X),\ x \mapsto (e_{G'}, x).$$

Alors η_X est bien G-équivariante, car pour tous $g \in G$ et $x \in X$, on a

$$\eta_X(g \cdot x) = (e_{G'}, g \cdot x) = (\phi(g), x) = \phi(g) \cdot (e_{G'}, x) = g * \eta_X(x).$$

(ii) pour un G'-ensemble Y, l'application ϵ_Y par

$$\epsilon_Y \colon (G' \times_{\phi} {}^{\phi}Y) \to Y,\ (g', y) \mapsto g' \cdot y.$$

Alors ϵ_Y est bien définie, car pour tous $g \in G$, $g' \in G'$ et $y \in Y$, on a

$$\epsilon_Y(g'\phi(g), y) = g'\phi(g) \cdot y = g' \cdot (\phi(g) \cdot y) = g' \cdot (g * y) = \epsilon_Y(g', g * y).$$

De plus, ϵ_Y est clairement G'-équivariante.

Finalement, on montre que les applications Φ et Ψ définie par

$$\Phi \colon \mathcal{F}_G(X, {}^{\phi}Y) \to \mathcal{F}_{G'}(G' \times_{\phi} X, Y),\ u \mapsto \epsilon_Y \circ \overline{u}$$

$$\Psi \colon \mathcal{F}_{G'}(G' \times_{\phi} X, Y) \to \mathcal{F}_G(X, {}^{\phi}Y),\ v \mapsto {}^{\phi}v \circ \eta_X$$

sont telles que $\Psi \circ \Phi = \mathrm{id}$ et $\Phi \circ \Psi = \mathrm{id}$. Soit $u \colon X \to {}^{\phi}Y$ G-équivariante. Alors $\Psi \circ \Phi(u)$ est donnée par la composition

$$\begin{array}{ccccccc} X & \xrightarrow{\eta_X} & {}^{\phi}(G' \times_{\phi} X) & \xrightarrow{{}^{\phi}\overline{u}} & {}^{\phi}(G' \times_{\phi} {}^{\phi}Y) & \xrightarrow{{}^{\phi}\epsilon_Y} & {}^{\phi}Y \\ x & \mapsto & (e_{G'}, x) & \mapsto & (e_{G'}, u(x)) & \mapsto & e_{G'} \cdot u(x) = u(x). \end{array}$$

Donc on a bien $\Psi \circ \Phi(u) = u$. Soit maintenant $v \colon G' \times_{\phi} X \to Y$ G'-équivariante. Alors $\Phi \circ \Psi(v)$ est donnée par la composition

$$\begin{array}{ccccccc} G' \times_{\phi} X & \xrightarrow{\overline{\eta_X}} & G' \times_{\phi} {}^{\phi}(G' \times_{\phi} X) & \xrightarrow{\overline{\phi_v}} & G' \times_{\phi} {}^{\phi}Y & \xrightarrow{\epsilon_Y} & Y \\ (g', x) & \mapsto & (g', (e_{G'}, x)) & \mapsto & (g', v(e_{G'}, x)) & \mapsto & g' \cdot v(e_{G'}, x) = v(g', x). \end{array}$$

Donc on a bien $\Phi \circ \Psi(v) = v$.

p-Sous-groupes de Sylow

Exercice 6. Soient p un nombre premier, G un groupe fini tel que p divise $|G|$, $P < G$ un p-sous-groupe de Sylow et $H < G$ un sous-groupe tel que $N_G(P) < H$. Montrer que $N_G(H) = H$.

Solution. Il est clair que $H < N_G(H)$. On montre que $N_G(H) < H$. Soit $g \in N_G(H)$. Alors, comme $P < N_G(P) < H$, on a que $gPg^{-1} < gHg^{-1} = H$. Comme $|H|$ divise $|G|$ et $P < H$, alors, si p^n est la plus grande puissance de p qui divise $|G|$, p^n est aussi la plus grande puissance de p qui divise H. Donc gPg^{-1} et P sont deux p-sous-groupes de Sylow de H. Comme tous les p-sous-groupes de Sylow sont conjugués entre eux, il existe $h \in H$ tel que $hgPg^{-1}h^{-1} = P$. Donc $hg \in N_G(P) < H$ et $g = h^{-1}(hg) \in H$, puisque $h^{-1}, hg \in H$. Donc on a bien $N_G(H) = H$.

Exercice 7. Soient p, q deux premiers distincts et G un groupe d'ordre $|G| = p^2q$.

(a) Montrer que G n'est pas simple.

(b) Montrer que, si $q < p$ et q ne divise pas $p^2 - 1$, alors G est abélien.

(c) En déduire que A_4 n'est pas simple et trouver tous les sous-groupes de Sylow de A_4.

Solution.

(a) Si $q < p$, alors un p-sous-groupe de Sylow P dans G est d'indice $[G : P] = q$, le plus petit nombre premier qui divise $|G|$. Donc il est normal par l'Exercice 4 (e) Série 5. Ainsi G n'est pas simple.

Si $p < q$, supposons par l'absurde que G soit simple. Alors le nombre n_q de q-sous-groupes de Sylow divise $|G| = p^2q$ et est tel que $n_q \equiv 1 (\text{mod } q)$. Donc $n_q \in \{1, p^2\}$, car on ne peut pas avoir $n_q = p$ puisque $n_q \equiv 1 (\text{mod } q$ et $q > p$. Comme G est simple, on a forcément $n_q = p^2$. Comme tous les q-sous-groupes de Sylow sont d'ordre q, ils sont cycliques et l'intersection de deux tels sous-groupes est forcément triviales. On compte alors $p^2 \cdot (q - 1) = p^2q - p^2$ éléments d'ordre q dans G. Il reste donc p^2 éléments dans G qui peuvent être d'un autre ordre et G ne peut donc contenir qu'un seul p-sous-groupe de Sylow (qui est d'ordre p^2). Donc le p-sous-groupe de Sylow est normal, par l'Exercice 3 (b) Série 10. Contradiction!

(b) Si $q < p$, on a vu en (a) que $n_p = 1$, car le p-sous-groupe de Sylow est normal, par l'Exercice 3 (b) Série 10. De plus, n_q est tel que n_q divise $|G| = p^2q$ et $n_q \equiv 1 (\text{mod } q)$, donc $n_q \in \{1, p, p^2\}$. Comme q ne divise pas $p^2 - 1$, alors $n_q \neq p$ et $n_q \neq p^2$. Donc $n_q = 1$ et G a un unique q-sous-groupe de Sylow. Par l'Exercice 6 Série 10, on a que $G \cong P \times Q$, où P est l'unique p-sous-groupe de Sylow et Q est l'unique q-sous-groupe de Sylow. De plus, par l'Exercice 2 (c) Série 10, P est abélien, car il est d'ordre p^2. Et Q est abélien, car cyclique d'ordre q. Donc G est abélien comme produit de groupes abéliens.

(c) On a que $|A_4| = 12 = 2^2 \cdot 3$. Donc, par (a), A_4 n'est pas simple. On cherche tous les 2- et 3-sous-groupes de A_4. On a que $n_2 \in \{1, 3\}$ et $n_3 \in \{1, 4\}$. Le sous-groupe $V = \{\text{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ est un 2-sous-groupe de Sylow de A_4 qui est normal. Par l'Exercice 3 (b) Série 10, on obtient que $n_2 = 1$. Donc V est le seul 2-sous-groupe de Sylow de A_4. Les 3-sous-groupes de Sylow sont quant à eux générés par un élément d'ordre 3 dans A_4, i.e. par un 3-cycle. On considère $\rho = (1\ 2\ 3)$. Alors, si $\sigma = (1\ 4)$, on a que

$$\sigma\rho\sigma^{-1} = (1\ 4)(1\ 2\ 3)(1\ 4) = (4\ 2\ 3) \notin \langle(1\ 2\ 3)\rangle.$$

Donc le 3-sous-groupe de Sylow $\langle(1\ 2\ 3)\rangle$ n'est pas normal dans A_4. Par l'Exercice 3 (b) Série 10, on obtient $n_3 = 4$ et les 3-sous-groupes de Sylow de A_4 sont donnés par

$$\langle(1\ 2\ 3)\rangle,\ \langle(1\ 3\ 4)\rangle,\ \langle(1\ 2\ 4)\rangle,\ \langle(2\ 3\ 4)\rangle.$$

Groupes libres

Exercice 8. Soit F un groupe libre de base X, où X est un ensemble.

(a) Pour $x \in X$, vérifier que l'application $s_x \colon F \to \mathbb{Z}$ qui envoie un mot réduit $w \in F$ sur la somme des exposants des termes x qui apparaissent dans w est un homomorphisme de groupes surjectif.

(b) Montrer que, si $w \in F$, alors $w \in [F, F]$ si et seulement si $s_x(w) = 0$ pour tout $x \in X$.

(c) Montrer que, si X est de rang fini $|X| = n > 2$, alors $F/[F, F] \cong \mathbb{Z}^n$.

Solution.

(a) Soit $w, w' \in F$ deux mots réduits. Comme la structure de groupe de F est donnée par la concaténation, il est clair que $s_x(ww') = s_x(w) + s_x(w')$. Donc s_x est bien un homomorphisme de groupes. De plus, si $n \in \mathbb{Z}$, alors $s_x(x^n) = n$. Cela montre que s_x est surjectif.

(b) Comme s_x est un homomorphisme et $\mathbb{Z}$ est abélien, alors $[F, F] \subset \mathrm{Ker}(s_x)$ pour tout $x \in X$. Donc si $w \in [F, F]$, on a bien $s_x(w) = 0$ pour tout $x \in X$. Soit maintenant $w \in F$ tel que $s_x(w) = 0$ pour tout $x \in X$. On écrit le mot w sous sa forme réduite

$$w = x_1^{n_1} \cdots x_r^{n_r}$$

avec $x_i \in X$ et $n_i \in \mathbb{Z}*$ pour tout $1 \leq i \leq k$. On montre par induction sur le nombre de termes r que $w \in [F, F]$. Si $r = 1, 2, 3$, alors il n'est pas possible d'avoir $s_x(w) = 0$ pour tout $x \in X$. Si $r = 4$, on doit avoir $x_1 = x_3$, $n_1 = -n_3$, $x_2 = x_4$ et $n_2 = -n_4$ puisque $s_{x_1}(w) = 0$ et $s_{x_2}(w) = 0$. Donc $w = [x_1^{n_1}, x_2^{n_2}] \in [F, F]$. Supposons maintenant que $r > 4$. Comme $s_{x_1}(w) = 0$, il existe $s \in \{1, \ldots, r\}$ tel que $x_s = x_1$. Alors

$$\begin{aligned} w = x_1^{n_1} \cdots x_r^{n_r} &= [x_1^{n_1}, x_2^{n_2} \cdots x_{s-1}^{n_{s-1}}] x_2^{n_2} \cdots x_{s-1}^{n_{s-1}} x_1^{n_1} x_s^{n_s} \cdots x_r^{n_r} \\ &= [x_1^{n_1}, x_2^{n_2} \cdots x_{s-1}^{n_{s-1}}] x_2^{n_2} \cdots x_{s-1}^{n_{s-1}} x_s^{n_1+n_s} x_{s+1}^{n_{s+1}} \cdots x_r^{n_r}, \end{aligned}$$

où $w' = x_2^{n_2} \cdots x_{s-1}^{n_{s-1}} x_s^{n_1+n_s} x_{s+1}^{n_{s+1}} \cdots x_r^{n_r}$ a $(r-1)$ termes. Par induction, $w' \in [F, F]$ et donc $w = [x_1^{n_1}, x_2^{n_2} \cdots x_{s-1}^{n_{s-1}}] w' \in [F, F]$.

(c) On écrit $X = \{x_1, \ldots, x_n\}$ et on considère l'application

$$\sigma = \prod_{i=1}^{n} s_{x_i} \colon F \to \mathbb{Z}^n,\ w \mapsto (s_{x_i}(w))_{i=1}^n.$$

C'est un homomorphisme de groupes surjectif, car chaque s_{x_i} est un homomorphisme de groupe surjectif par le point (a). Alors $\sigma(w) = 0$ si et seulement si $s_{x_i}(w) = 0$ pour tout $1 \leq i \leq n$ si et seulement si $w \in [F, F]$ par le point (b). Donc $\mathrm{Ker}(\sigma) = [F, F]$ et, par le premier théorème d'isomorphisme $F/[F, F] \cong \mathbb{Z}^n$.