TD ACCQ 201

Julien Béguinot, Duong Hieu Phan

Télécom Paris

1 Rappels

1.1 Définitions Essentiels

Definition 1. Soit G un groupe et H un sous-groupe de G. On dit que H est **distingué** dans G et on note $H \lhd G$ si $\forall g \in G, gH = Hg$. En d'autre termes les classes à droites et les classes à gauches de H dans G coincident.

Definition 2. Un groupe engendré par un seul élément est dit **monogène**. Un groupe monogène et fini est dit **cyclique**.

Definition 3. Le **centre** $\mathcal{Z}(G)$ est l'ensemble des éléments de G commutants avec tous les éléments de G. Pour x un élément de G le centralisateur de x dans G est l'ensemble des éléments de G commutant avec x.

Definition 4. Soit X un ensemble et G un groupe. On dit que G **agit** sur X s'il existe une fonction (une action de groupe): $\begin{cases} X \times G \mapsto G \\ (x, g) \mapsto g \cdot x \end{cases}$ tel que $(i) : \forall (s, g) \in G^2, \forall x \in X, s \cdot (g \cdot x) = (sg) \cdot x$ et $(ii) : e \cdot x = x$. On note $\mathcal{O}_x = \{g \cdot x | g \in G\}$ l'**orbite** de x et $\mathcal{S}_x = \{g \in G | g \cdot x = x\}$ le **stabilisateur** de x.

Definition 5. On appele **indicatrice d'Euler** noté $\varphi : \mathbb{N}^* \mapsto \mathbb{N}^*$ l'application qui donne l'ordre du groupe des inversibles (pour $\times$) de $\mathbb{Z}_n$. C'est une fonction multiplicative et on peut monter que si $N = \prod p_i^{\nu_i}$ alors

$$\varphi(N) = \prod p_i^{\nu_i - 1}(p_i - 1)p_i^{\nu_i - 1} = N \prod \left(1 - \frac{1}{p_i}\right).$$

1.2 Résultats Principaux

Lemma 1 (Lagrange)**.** *Soit G un groupe fini et H un sous-groupe de G. Alors l'ordre de H divise l'ordre de G. En particulier il existe un entier noté $[G : H]$ apppelé ordre de H dans G tel que*

$$|G| = [G : H]|H|.$$

Lemma 2 (Equation aux Classes)**.** *Soit X un ensemble et G un groupe fini agissant sur X. Alors pour tout x de X,*

$$|G| = |\mathcal{O}_x||\mathcal{S}_x|.$$

En particulier en prenant un representant de chaque orbite dans un ensemble Θ on partitione X est donc

$$|X| = \sum_{x \in \Theta} |\mathcal{O}_x|.$$

Lemma 3 (Formule de Burnside)**.** *Soit G un groupe agissant sur l'ensemble X,*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$$

où $\mathrm{Fix}(g) = \{x \in X | g \cdot x = x\}$ *est l'ensemble des points fixe de X sous l'action de l'élement g.*

Theorem 1 (Caractérisation des Groupes Cycliques)**.** *Soit G un groupe cyclique d'ordre n on a*

$$G \simeq \mathbb{Z}_n.$$

Theorem 2 (Théorème des Restes Chinois)**.** *Soit $n = \prod_{i=1}^{d} n_i$ avec $n_1, \ldots, n_d$ premiers deux à deux. Alors*

$$\theta : \begin{cases} \mathbb{Z}_n \mapsto \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_d} \\ x[n] \mapsto (x[n_1], \ldots, x[n_d]) \end{cases}$$

est un isomorphise d'anneaux.

Theorem 3. *Soit $n \in \mathbb{N}^*$,*

$$n = \sum_{d|n} \varphi(d).$$

Theorem 4 (Structure des Groupes Abéliens Finis)**.** *Soit G un groupe abélien fini d'odre N. Il existe une unique suite $d_r \geqslant \ldots \geqslant d_1 > 1$ avec $d_i | d_{i+1}$ tel que*

$$G \simeq \mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_r}.$$

Les entiers $d_1, \ldots, d_r$ sont appelés les ***invariants*** *du groupe (et caractérisent donc le groupe à isomorphisme près).*

2 Exercices

Exercice 1 (Inverse du TRC)**.** *D'après le TRC $\theta : \mathbb{Z}_{35} \mapsto \mathbb{Z}_5 \times \mathbb{Z}_7$ est un isomorphisme. Construire explicitement son inverse θ^{-1}.*

Solution 1. Clairement $\theta^{-1}(x, y) = 7 * (7^{-1}[5])x + 5 * (5^{-1}[7])y$ donne l'inverse. Il suffit donc de retrouver les inverses. Or $-2 * 7 + 3 * 5 = 1$. Finalement, $\theta^{-1}(x, y) = -14x + 15y$ convient.

Exercice 2. *Soit G un groupe abélien d'ordre 60. Décrire à isomorphisme prêt les structures possible pour G.*

Solution 2. Par application direct du théorème de structure on obtient deux possibilités à savoir $\mathbb{Z}_2 \times \mathbb{Z}_{30}$ ou Z_{60}.

Exercice 3 (Centre et Abélianité)**.** *Soit G un groupe de centre Z.*

- *Montrer que $Z \lhd G$*
- *Montrer que si G/Z est monogène alors G est abélien.*

Solution 3. Comme G/Z est monogène on dispose de g dans G tel que $G/Z = \{\bar{g}^k | k \in \mathbb{Z}\}$. Soit x, y deux éléments de G. On a $\bar{x} \in G/Z$ donc $x = g^i z_1$ pour un certain entier i et un $z_1 \in Z$. De même $y = g^j z_j$ pour un certain entier j et un $z_j \in Z$. Puis $xyx^{-1} = g^i z_1 g^j z_2 z_1^{-1} g^{-i} = g^j z_2 = y$.

Exercice 4 (Lemme de Cauchy)**.** *Soit G un groupe fini dont l'ordre est un multiple de p un nombre premier. Montrer que G admet un élément d'ordre p.*

Solution 4. On fait agir $\mathbb{Z}_p$ sur l'ensemble $A = \{(x_1, \dots, x_p) | x_1 \dots x_p = e\}$. Alors chaque orbite contient ou bien 1 élément si $x_1 = \dots = x_p$ ou p éléments sinon. On note r, N le nombre de tel orbite. Alors $|A| = r + Np$. Mais d'autres par $|A| = |G|^{p-1}$ donc il vient que $p|r$ et donc $r > 1$.

Exercice 5. *Soit G un groupe fini d'ordre p ou p^2 avec p premier. Montrer que G est abélien. En déduire l'ensemble des structures possibles pour G à isomorphisme près.*

Solution 5. Si $G \simeq \mathbb{Z}_p$ est d'ordre p alors il est cyclique donc abélien. Si G est d'ordre p^2 alors on considére son centre Z. Si Z est d'ordre p^2 on a fini. D'après l'équation aux classes Z ne peut pas être d'ordre 1 (Considérer l'action de conjugaison de G sur G). Si Z est d'ordre p alors G/Z est d'ordre p. Mais alors d'après l'exercice 3, G est abélien ce qui est absurde. On a donc deux structure possible $\mathbb{Z}_{p^2}$ ou $\mathbb{Z}_p^2$.

Exercice 6 (Théorème du Rang)**.** *Soit G un groupe et $f : G \mapsto G$ un endomorphisme. Montrer que*

$$|G| = |\mathrm{Ker} f||\mathrm{Im} f|.$$

Solution 6.

$$\begin{aligned} |G| &= \sum_{y \in \mathrm{Im(f)}} |f^{-1}(\{y\})| && (1)\\ &= \sum_{y \in \mathrm{Im(f)}} |f^{-1}(y)\mathrm{Ker}(f)| && (2)\\ &= \sum_{y \in \mathrm{Im(f)}} |\mathrm{Ker}(f)| && (3)\\ &= |\mathrm{Ker} f||\mathrm{Im} f| && (4) \end{aligned}$$

Exercice 7. *Soit G un groupe abélien d'ordre pq avec p, q deux nombres premiers. Montrer que G est un groupe cyclique. Et si G n'est pas abélien ?*

Solution 7. D'après le théorème de Cauchy on dispose de g_1, g_2 d'ordre p, q respectivement. Soit $g = g_1 g_2$ alors g est d'ordre pq. En effet, il ne peut pas etre d'odre p (ou q) car $g^p = g_1^p g_2^p = e g_2^p = g_2^p \neq e$. Si G n'est pas abélien cela ne fonctionne plus, par exemple le groupe des symétries du triangle équilatérale est d'ordre $6 = 2 \times 3$ mais n'est pas cyclique.

Exercice 8. *Combien y-a-t'il de collier de perles* ***différents*** *formés à partir de 4 perles rouges et 4 perles bleu ?*

Solution 8. On propose une solution élégante à l'aide de la formule de Burnside. On cherche $|X/\mathbb{Z}_8|$ avec X l'ensemble des octuplets contenant 4 fois la valeur B et 4 fois la valeur R. On a $|4| = \binom{8}{4}$. Puis on applique la formule de Burnside. Si $g = \bar{0}$ on a $|\mathrm{Fix}(g)| = |X|$. Si $g = \bar{1}, \bar{-1}, \bar{3}, \bar{-3}$ on a $|\mathrm{Fix}(g)| = 0$. Si $g = \bar{2}, \bar{-2}$ on a $|\mathrm{Fix}(g)| = 2$. Finalement si $g = \bar{4}$ on a $|\mathrm{Fix}(g)| = 6$. Ainsi d'après la formule de Burnside $|X/\mathbb{Z}_8| = (70+2+2+6)/8 = 80/8 = 10$. Il n'y a donc que 10 colliers distincts.

Exercice 9. *Soit G un groupe et H_1, H_2 deux sous-groupes de G. Il est connu que $H_1 \cap H_2$ est un sous-groupe de G. Qu'en est-il de $H_1 \cup H_2$?*

Solution 9. On montre que $H_1 \subset H_2$ ou inversement. Supposons qu'il n'y ai pas de tel relation d'inclusion. Alors il existe au moins un élement g_1 de H_1 qui n'est pas dans H_2 et un élément g_2 de H_2 qui n'est pas dans H_1. Mais alors $g = g_1 g_2$ n'est ni dans H_1 ni dans H_2 donc n'est pas dans $H_1 \cup H_2$. Ainsi ce n'est pas un sous-groupe.

Exercice 10. *Soit G, H, L des groupes tels que $L \lhd H$ et $H \lhd G$. A-t-on $L \lhd G$?*

Solution 10. Ce n'est pas vrai en général. On peut prendre un contre exemple. Par exemple $G = \mathcal{S}_4$, $L = \langle 1, (1,2)(3,4)\rangle$ and $H = \langle 1, (1,2)(3,4), (1,3)(2,4)\rangle$.