Sous-groupes distingués et groupes quotients

Travaux dirigés du 30 septembre et du 3 octobre 2025

Exercice 1. Manipulations de quotients

1. Soient H un sous-groupe distingué d'indice fini n de G, et $g \in G$. Montrer $g^n \in H$.
2. Montrer que si G est un groupe tel que $G/Z(G)$ est monogène, alors G est abélien.
3. Soient $(G_i)_{i\in I}$ une famille de groupes et, pour tout $i \in I$, H_i un sous-groupe distingué de G_i. On pose $G = \prod_{i\in I} G_i$, $H = \prod_{i\in I} H_i$. Montrer que H est distingué dans G, et qu'on a un isomorphisme naturel $G/H \simeq \prod_{i\in I} G_i/H_i$.

Exercice 2. Deuxième théorème d'isomorphisme

Soit G un groupe, soit H un sous-groupe de G et soit N soit un sous-groupe du normalisateur de H (on dit que N *normalise* H).

1. Montrer que NH est un sous-groupe de G.
2. Montrer que H est distingué dans NH et $N \cap H$ est distingué dans N.
3. Montrer que $N/N\cap H \to NH/H$, $n(N\cap H) \mapsto nH$ est un isomorphisme.

Exercice 3. Premier théorème de Sylow

Soit G un groupe fini d'ordre $p^n m$ avec p premier ne divisant pas m et $n \geq 1$. Pour $x \in G$, on note $\mathrm{Conj}(x)$ la classe de conjugaison de x et $\mathrm{C}_G(x)$ son commutant.

1. Montrer que s'il existe $x \in G - Z(G)$ tel que $|\mathrm{Conj}(x)|$ est premier à p, alors on peut trouver un sous-groupe de G de cardinal $p^n m'$ avec $m' < m$.
2. Montrer que si $p||\mathrm{Conj}(x)|$ pour tout $x \in G - Z(G)$, alors on peut trouver un sous-groupe de G de cardinal p et distingué dans G.
3. *(Premier théorème de Sylow)* Montrer que G possède un sous-groupe d'ordre p^n. Un tel sous-groupe s'appelle un p*-Sylow* de G.

Exercice 4. Simplification par un groupe

Soient G, H et K des groupes finis. On se propose de montrer que si on a $G \times H \simeq G \times K$, alors on a $H \simeq K$. Pour deux groupes X, Y, on notera $\mathrm{Inj}(X,Y) \subseteq \mathrm{Hom}(X,Y)$ le sous-ensemble des morphismes injectifs.

1. Montrer que pour tout groupe fini S, on a $|\mathrm{Hom}(S,H)| = |\mathrm{Hom}(S,K)|$.
2. En déduire que pour tout groupe fini S, on a $|\mathrm{Inj}(S,H)| = |\mathrm{Inj}(S,K)|$.
3. Conclure.
4. Donner un exemple de groupe infini G vérifiant $G \times \mathbb{Z}/2\mathbb{Z} \simeq G \simeq G \times G$.

Exercice 5. Disgression arithmétique

Dans l'exercice 4 du TD précédent, on a vu que les sous-groupes du groupe des inversibles d'un corps étaient cycliques. Il en découle que pour p premier, $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique. Maintenant, on va regarder la structure de $(\mathbb{Z}/n\mathbb{Z})^\times$ pour n quelconque. D'après l'isomorphisme chinois, il suffit de traiter le cas où n est une puissance d'un nombre premier.

1. Soit $k \geq 0$ un entier. Montrer que si p est un nombre premier impair, alors $(1+p)^{p^k} \equiv 1 + p^{k+1}[p^{k+2}]$. Montrer également $(1+4)^{2^k} \equiv 1 + 2^{k+2}[2^{k+3}]$.
2. Soit p premier impair et $m \geq 1$. Montrer que le groupe $(\mathbb{Z}/p^m\mathbb{Z})^\times$ est cyclique.
3. Soit $m \geq 2$. Montrer qu'on a $(\mathbb{Z}/2^m\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}$.

Exercice 6. En général, on ne peut vraiment rien dire sur l'ordre du produit de deux éléments

Dans l'exercice 5 du TD précédent, on a vu le résultat suivant :

Proposition. *Pour tous entiers $a, b, c \geq 3$ (avec éventuellement $c = \infty$), il existe un groupe fini possédant un élément d'ordre a et un autre d'ordre b, dont le produit est d'ordre c.*

On rappelle que l'on avait en fait montré l'existence d'un corps fini k avec $\mathrm{car}(k) \neq 2$ tel que le groupe $SL_2(k)$ convienne. En se plaçant dans le groupe quotient $SL_2/\{\pm 1\}$, généraliser la proposition à tout $a, b, c \geq 2$.

Exercice 7. Groupes libres et présentations de groupes

Soit X un ensemble fini. Pensons à X comme à un alphabet et définissons l'ensemble des *mots* sur X comme étant

$$\mathrm{Mots}(X) = \coprod_{n\geq 0} X^n$$

Par convention, on a posé ici $X^0 = \{1\}$, et on note aussi $\emptyset$ son unique élément, appelé *mot vide*. Un élément de $X^n \subset \mathrm{Mots}(X)$ sera appelé *mot de longueur n* sur X, et on notera simplement $x_1 \cdots x_n$ le n-uplet $(x_1, \cdots, x_n)$. On définit une loi de composition sur $\mathrm{Mots}(X)$ par la concaténations des mots :

$$X^n \times X^m \to X^{n+m}, \left(x_1 \cdots x_n, y_1 \cdots y_m\right) \mapsto x_1 \cdots x_n y_1 \cdots y_n.$$

1. Vérifier que $\mathrm{Mots}(X)$ est un monoïde et qu'on a une inclusion $X \subseteq \mathrm{Mots}(X)$.
2. *(Propriété universelle de l'ensemble des mots)* Montrer que pour tout monoïde M, toute application $X \to M$ s'étend de manière unique en un morphisme de monoïdes $\mathrm{Mots}(X) \to M$.

On pose maintenant $X^{\pm} = X \coprod X$. On a l'inclusion à gauche (resp. à droite) $X \subseteq X^{\pm}$. Tout élément $x \in X^{\pm}$ dans la copie de X à gauche (resp. droite) a un correspondant que l'on notera x^{-1} dans celle de droite (resp. de gauche). Soit R la relation sur $\mathrm{Mots}\left(X^{\pm}\right)$ telle que deux mots sont équivalents si et seulement si l'un s'obtient à partir de l'autre après une suite finie d'insertions ou suppressions de morceaux de la forme xx^{-1} avec $x \in X^{\pm}$.

3. Vérifier que R est une relation d'équivalence. On note l'ensemble quotient associé $\mathrm{F}_X = \mathrm{Mots}\left(X^{\pm}\right)/R$, et on notera $[m]$ la classe d'équivalence de m.
4. Montrer qu'il existe une unique loi de monoïde sur F_X telle que la projection canonique $\mathrm{Mots}\left(X^{\pm}\right) \to \mathrm{F}_X$ est un morphisme de monoïde.
5. Montrer que cette loi fait de F_X un groupe engendré par les $[x]$ avec $x \in X$. On dit que F_X est le *groupe libre* sur X.
6. *(Propriété universelle du groupe libre)* Montrer que pour tout groupe G et pour toute application $f : X \to G$, il existe un unique morphisme de groupes $f' : \mathrm{F}_X \to G$ tel que $f'([x]) = f(x)$ pour tout $x \in X$.
7. Un mot sur $X^{\pm}$ est dit *réduit* s'il est vide ou de la forme $x_1 \ldots x_n$ avec $x_i \in X^{\pm}$ pour $1 \leq i \leq n$ et $x_{i+1} \neq x_i^{-1}$ pour $1 \leq i < n$. Montrer que l'application canonique $\mathrm{Mots}\left(X^{\pm}\right) \to \mathrm{F}_X, m \mapsto [m]$, induit une bijection entre le sous-ensemble des mots réduits sur $X^{\pm}$ et F_X. En particulier, l'application naturelle $X^{\pm} \to \mathrm{F}_X, x \mapsto [x]$, est injective ; souvent, on notera simplement x la classe $[x]$ en voyant $X^{\pm}$ comme une partie de F_X.
8. Décrire F_X pour $X = \emptyset$ et pour $X = \{x\}$ un singleton. Montrer que pour $|X| \geq 2$, le groupe F_X est non commutatif.
9. Montrer que toute application $X \to Y$ (resp. bijection) induit un morphisme (resp. isomorphisme) de groupes $\mathrm{F}_X \to \mathrm{F}_Y$. Un groupe G est dit *libre* s'il est isomorphe à F_X pour un certain X. Pour $n \geq 1$, on note F_n un groupe libre sur un ensemble à n éléments.

On discute maintenant de la notion de groupe défini par générateurs et relations. Soient G un groupe ainsi que $\{g_x\}_{x\in X}$ une famille d'éléments de G indexée par un ensemble X. Par propriété universelle du groupe libre, il existe un unique morphisme de groupes $f : \mathrm{F}_X \to G$, avec $f(x) = g_x$ pour tout $x \in X$. On dit alors qu'un mot $m \in \mathrm{Mots}\left(X^{\pm}\right)$ est une *relation* entre les g_x si on a $f([m]) = 1$. Comme tout mot m' équivalent à une relation m entre les g_x est encore une relation entre les g_x, on dira aussi que $[m] \in \mathrm{F}_X$ est une *relation* entre les g_x. L'ensemble de toutes les relations entre les g_x est donc $\ker f \subseteq \mathrm{F}_X$. Comme les $x \in X$ engendrent F_X, le morphisme f est surjectif si et seulement si les g_x engendrent G, auquel cas on a $\mathrm{F}_X/\ker f \simeq G$.

10. Donner des exemples de relations vérifiées par un groupe commutatif, puis un groupe d'ordre n, puis $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.
11. Montrer que pour toute partie X d'un groupe G, il existe un plus petit sous-groupe distingué de G contenant X, à savoir le sous-groupe engendré par $\cup_{g\in G} gXg^{-1}$. C'est la *clôture normale* de X dans G, on la note $\langle X\rangle^{\triangleleft}$.

Soient $\mathscr{G}$ un ensemble et $\mathscr{R} \subset \mathrm{Mots}\left(\mathscr{G}^{\pm}\right)$ un sous-ensemble. Le groupe quotient $\mathrm{F}_{\mathscr{G}}/\langle\mathscr{R}\rangle^{\triangleleft}$ est appelé *groupe défini par les générateurs $\mathscr{G}$ et par les relations $\mathscr{R}$* ; on le note aussi $\langle \mathscr{G} \mid r = 1, \forall r \in \mathscr{R}\rangle$. Étant donné un groupe G, un isomorphisme $\langle \mathscr{G} \mid r = 1, \forall r \in \mathscr{R}\rangle \xrightarrow{\sim} G$ s'appelle une *présentation* de G (par les générateurs $\mathscr{G}$ et les relations $\mathscr{R}$). Lorsque $\mathscr{G}$ et $\mathscr{R}$ sont finis, disons $\mathscr{G} = \{g_1, \ldots, g_n\}$ (tous distincts) et $\mathscr{R} = \{r_1, \ldots, r_s\}$, on le note aussi $\langle g_1, \ldots, g_n \mid r_1 = r_2 = \cdots = r_s = 1\rangle$ et on parle de *présentation finie*.

12. *(Propriété universelle d'un groupe défini par générateurs et relations)* Soient $\mathscr{G}$ un ensemble, $\mathscr{R} \subset \mathrm{Mots}\left(\mathscr{G}^{\pm}\right)$ et G un groupe. Montrer qu'il est équivalent de se donner un morphisme de groupes $\langle \mathscr{G} \mid r = 1, \forall r \in \mathscr{R}\rangle \to G$ et une application $f : \mathscr{G} \to G$ telle que $f(r) = 1$ pour tout $r \in \mathscr{R}$.
13. Montrer que μ_n admet la présentation $\langle a \mid a^n = 1\rangle$ et $\mathbb{Z} \times \mathbb{Z}$ la présentation $\langle a, b \mid aba^{-1}b^{-1} = 1\rangle$.
14. Montrer que tout groupe fini admet une présentation finie.