Exercices pour se familiariser avec les groupes

En TD, la sélection d'exercices vise à vous faire comprendre des méthodes ou des idées classiques gravitant autour des cours de la semaine. Ce document vise à fournir une petite liste d'exercices pour se familiariser d'abord avec le cours. Il s'agira d'énoncés dont les preuves nécessitent uniquement de connaître les définitions ou faire quelques calculs basiques, ce qui est toujours important pour s'habituer à de nouveaux objets. Le document est découpé suivant les TDs et propose trois ou quatre exercices par semaine de cours. Comme d'habitude, n'hésitez pas à m'envoyer un mail à nataniel.marquis@dma.ens.fr ou à venir me poser les questions directement au bureau T13.

FIGURE 1 – Devenez aussi familier·ère avec les groupes que la druide avec cet ourson !

TD n°1 : Relations

Exercice 1.

Démontrer que les relations suivantes sont d'équivalence :

1. Soit $N \geq 1$ un entier. Considérer la relation de congruence sur $\mathbb{Z}$ définie par
$$a \equiv b \text{ ssi } n|(a-b).$$
2. Pour un ensemble E, considérer la relation sur ses parties $\mathcal{P}(E)$ définie par
$$A\mathcal{R}B \text{ ssi } (A = B) \text{ ou } (A = \overline{B}).$$
3. Soit X un ensemble et $f : X \to X$ une bijection. Considérer la relation d'orbite définie par
$$x\mathcal{O}y \text{ ssi } \exists i \in \mathbb{Z},\ f^{\circ i}(x) = y.$$

Exercice 2.

Soit $N \geq 1$ un entier. Nous considérons de nouveau la relation de congruence $\equiv$ définie sur $\mathbb{Z}$ comme au premier exercice.

1. Décrire les classes d'équivalences.
2. On appelle $\mathbb{Z}/N\mathbb{Z}$ l'ensemble quotient. Écrire explicitement la projection canonique
$$\pi_{\equiv} : \mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}.$$
3. Soit ζ une racine n-ième de l'unité dans $\mathbb{C}$. Considérons l'application
$$f : \mathbb{Z} \to \mathbb{C}^\times,\ n \mapsto \zeta^n.$$
Démontrer qu'elle se factorise par la projection canonique $\pi_{\equiv}$, au sens où il existe une unique application $g : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}^\times$ telle que $f = g \circ \pi_{\equiv}$.

Exercice 3.

Nous allons étudier la relation de contraction d'une partie.

1. Soit X un ensemble et $Z \subset X$. On définit la relation de contraction par
$$x\mathcal{R}_Z y \text{ ssi } \left((x,y) \in Z^2 \text{ ou } x = y\right).$$
Vérifier qu'il s'agit d'une relation d'équivalence.
2. Considérons le segment $[0,1]$ et sa partie $\{0,1\}$. Considérons l'application
$$f : [0,1] \to \mathbb{C}^\times,\ x \mapsto e^{2i\pi x}.$$
Vérifier qu'elle se factorise par la projection canonique associée à $\mathcal{R}_{\{0,1\}}$ puis que la factorisation obtenue est une bijection de $[0,1]/\mathcal{R}_{\{0,1\}}$ sur le cercle unité de $\mathbb{C}$.
3. Faire un dessin joli et concis.

Exercice 4.

1. Soit X un ensemble, I un ensemble totalement ordonné et $(\mathcal{R}_i)_{i\in I}$ une famille relation d'équivalences sur X, croissante au sens où $\mathcal{R}_i \subseteq \mathcal{R}_j$ dès que $i \leq j$. Vérifier que $\cup_{i\in I}\mathcal{R}_i$ est une relation d'équivalence.
2. Soit X un ensemble et $\mathfrak{E}$ un sous-ensemble de X^2 n'intersectant pas la diagonale $\{(x,x)\,|\,x\in X\}$. Démontrer qu'il existe une relation d'équivalence maximale disjointe de $\mathfrak{E}$. On pourra considérer l'ensemble

$$\{\mathcal{R}\subset X^2\,|\,\text{relation d'équivalence telle que } \mathcal{R}\cap\mathfrak{E}=\emptyset\}$$

muni de l'inclusion et vérifier qu'il est inductif.

TD n°2 : Groupes et groupes cycliques

Exercice 1.

Soit $f : G \to G'$ un morphisme de groupes [1].

1. Démontrer que $f(1_G) = 1_{G'}$ et que pour tout $x \in G$, nous avons $f(x^{-1}) = f(x)^{-1}$.
2. Soit H un sous-groupe de G. Démontrer que $f(H)$ est un sous-groupe de G'.

Exercice 2.

Dans chacun des cas suivants, vérifier que H est un sous-groupe de G, puis que l'application explicite est un isomorphisme de groupes.

1. Soit $n \geq 1$. On considère $G = \mathfrak{S}_n$ et $H = \{\sigma \in \mathfrak{S}_n\,|\,\sigma(n) = n\}$. L'application sera

$$\mathfrak{S}_{n-1} \to H,\ \ \tau \mapsto [k \mapsto \tau(k) \text{ si } k < n \text{ et } n \mapsto n].$$

2. Soit $n \geq 1$ et $k \leq n$ On considère $G = \mathfrak{S}_n$ et

$$H = \{\sigma \in \mathfrak{S}_n\,|\,\forall i \leq k,\ \sigma(i) \leq k\}.$$

L'application sera

$$\mathfrak{S}_k \times \mathfrak{S}_{n-k} \to H,\ \ (\sigma_1,\sigma_2) \mapsto \left[i \mapsto \left\{ \begin{array}{ll} \sigma_1(i) & \text{si } i \leq k \\ k+\sigma_2(i-k) & \text{si } i > k \end{array} \right.\right].$$

1. À ce stade défini par $\forall (x,y)\in G^2,\ \ f(xy) = f(x)f(y)$.

Exercice 3.

Soit $n \geq 1$ et $\zeta \in \mathbb{C}^\times$ une racine primitive n-ième de l'unité (i.e. un élément d'ordre n du groupe multiplicatif $\mathbb{C}^\times$).

1. Vérifier que le groupe des racines n-ièmes de l'unité $\mu_n = \{z \in \mathbb{C}^\times \,|\, z^n = 1\}$ est un sous-groupe du groupe multiplicatif $\mathbb{C}^\times$. Démontrer en considérant le polynôme $X^n - 1$ qu'il possède au plus n éléments.
2. On rappelle par définition de l'ordre d'un élément que
$$\mathbb{Z} \to \mathbb{C}^\times, \;\; k \mapsto \zeta^k$$
est un morphisme de groupe de noyau $n\mathbb{Z}$. En déduire un isomorphisme de groupe
$$\mathbb{Z}/n\mathbb{Z} \to \mu_n.$$
3. Retrouver que $\mathbb{Z}/n\mathbb{Z}$ possède des éléments d'ordre d pour tout diviseur d de n.

Exercice 4.

1. Soit $f : G_1 \hookrightarrow G_2$ un morphisme de groupes injectif et $g_1 \in G_1$. Démontrer que l'ordre de $f(g_1)$ coïncide avec celui de g_1.
2. Soit G un groupe et $g \in G$ un élément d'ordre fini n. Vérifier que l'application
$$\mathbb{Z} \to G, \;\; k \mapsto g^k$$
est un morphisme de groupe de noyau $n\mathbb{Z}$. En déduire qu'elle se factorise en un morphisme de groupes injectif de $\mathbb{Z}/n\mathbb{Z}$ dans G.
3. En utilisant l'exercice 3, déduire que G contient un élément d'ordre d pour tout diviseur d de n.

TD n°3 : Quotients et groupes usuels

Exercice 1.

Soit G un groupe et $H \triangleleft G$ un sous-groupe distingué. Nous notons $\pi : G \to G/H$ la projection sur le groupe quotient.

1. Vérifier que les applications
$$\begin{aligned} \{H' \text{ sous-groupe de } G \text{ tel que } H \subset H'\} &\rightleftarrows \left\{K \text{ sous-groupe de } G/H\right\}, \\ H' &\mapsto \pi(H') \\ \pi^{-1}(K) &\hookleftarrow K \end{aligned}$$
sont bien définies et inverses l'une de l'autre.
2. Rappeler pourquoi les sous-groupes de $\mathbb{Z}$ sont exactement les $d\mathbb{Z}$ pour $d \geq 0$. Vérifier que $d_1\mathbb{Z}$ est sous-groupe de $d\mathbb{Z}$ ssi $d|d_1$.
3. Retrouver la liste des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.

Exercice 2.

Soit G un groupe.

1. En considérant le sous-groupe $\langle (1\,2), (3\,4)\rangle$ dans $\langle (1\,2\,3\,4), (1\,2)\rangle$, démontrer qu'un sous-groupe distingué K d'un sous-groupe distingué H de G n'est pas nécessairement distingué dans G.

On dit qu'un sous-groupe H de G est *caractéristique* si tout automorphisme φ de G stabilise H (i.e. $\varphi(H) = H$).

1. Soit H un sous-groupe distingué de G. Démontrer qu'un sous-groupe caractéristique K de H est distingué dans G.
2. Soit G un groupe abélien et n un entier. Démontrer que les sous-ensembles $nG = \{ng \,|\, g \in G\}$ et $G[n] = \{g \in G \,|\, ng = 0_G\}$ sont des sous-groupes caractéristiques de G.

Exercice 3.

Soit G un groupe.

1. Supposons G abélien. Soit $G_{\text{tors}} = \{g \,|\, \exists n \geq 1,\ g^n = 1\}$. Vérifier que G_{tors} est un sous-groupe de G puis que tout élément de G/G_{tors} est d'ordre infini.
2. Supposons G abélien fini. Soit p un nombre premier et $G[p^\infty] = \{g \,|\, \exists n \geq 1,\ g^{p^n} = 1\}$. Vérifier que $G[p^\infty]$ est un sous-groupe de G puis que tout élément de $G/G[p^\infty]$ est d'ordre premier à p.
3. Soit $n \geq 2$. On considère $G^{(n)}$ le sous-groupe de G engendré par $\{g^n \,|\, g \in G\}$. Démontrer que $G^{(n)}$ est un sous-groupe distingué de G puis que $G/G^{(n)}$ est un groupe de n-torsion [2]

Exercice 4.

1. Redémontrer que les sous-groupes de $\mathbb{R}$ sont denses ou de la forme $\alpha\mathbb{Z}$ pour un certain réel $\alpha \geq 0$.
2. Soit x un irrationnel. Vérifier que 1 et x ne peuvent être multiples entiers d'un même réel. En conclure que $\mathbb{Z} + x\mathbb{Z}$ est dense dans $\mathbb{R}$.

Exercice 5.

Soit G un groupe, $N \triangleleft G$ un sous-groupe distingué et $H < G$ un sous-groupe. Démontrer que l'ensemble $NH = \{nh \,|\, n \in N,\, h \in H\}$ est un sous-groupe de G.

TD n°4 : Groupes abéliens

Exercice 1.

Cet exercice classe dans un premier temps les groupes abéliens d'ordre 27 à isomorphisme près.

2. Cela signifie que l'ordre de tout élément divise n.

1. Décomposer 27 en facteurs premiers.
2. Trouver les suites $d_1|d_2|\dots|d_n$ d'entiers se divisant telles que $\prod_i d_i = 27$. On pourra commencer par séparer les telles suites selon le diviseur d_n de 27.
3. Utiliser le théorème de classification des groupes abéliens finis pour trouver des représentants des classes d'isomorphismes de groupes abéliens d'ordre 27.

Nous continuons en choisissant $p_1, \dots, p_k$ des premiers distincts.

1. Démontrer que la seule suite $d_1|\dots|d_n$ telle que $\prod_i d_i = \prod_{j\leq k} p_j$ est $\prod_{j\leq k} d_j$.
2. En déduire qu'il n'existe qu'une classe d'isomorphisme de groupes abéliens d'ordre $\prod_{j\leq k} p_j$.

Exercice 2.

Nous considérons le groupe $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

1. Quels sont les éléments d'ordre 1, 2 et 4 de G ?
2. Trouver les sous-groupes de G. On pourra distinguer selon le cardinal et l'ordre maximal d'un élément du sous-groupe.

Exercice 3.

Cet exercice s'intéresse aux caractères d'ordre 2 des groupes abéliens finis. Il s'intéresse ensuite au cas des $(\mathbb{Z}/p\mathbb{Z})^\times$ pour retrouver le symbole de Legendre.

Soit G un groupe cyclique, noté multiplicativement. On pourra reprendre l'exercice avec G abélien fini quelconque avec les modifications en bleu.

1. Soit $G^{(2)}$ l'ensemble des carrés des éléments de G. Démontrer que $G^{(2)}$ est un sous-groupe de G.
2. Démontrer qu'un élément d'ordre impair est un carré.
3. En déduire que $G^{(2)} = G$ si tout élément de G est d'ordre impair, et que $[G : G^{(2)}] = 2$ sinon. On démontrera que $[G : G^{(2)}]$ vaut le nombre d'éléments de carré trivial.
4. Soit χ un caractère de G d'ordre 2, i.e. tel que $\chi^2 = 1$. Démontrer que $\mathrm{Im}(\chi) \subseteq \{\pm 1\}$, puis que $G^{(2)}$ est contenu dans le noyau de χ.
5. En déduire que χ est trivial ou, dans le cas où $[G : G^{(2)}] = 2$, identifié à la projection sur de $G/G^{(2)}$. En notant χ_2 ce caractère, on démontrera que le noyau de χ_2 est précisément l'ensemble des carrés de G. Démontrer que l'ensemble des carrés de G est l'intersection des noyaux des caractères d'ordre 2.

Nous cherchons à présent à appliquer cela à $(\mathbb{Z}/p\mathbb{Z})^\times$ pour $p \neq 2$.

1. Soit $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. Rappeler pourquoi $a^{p-1} = 1$ puis démontrer que $a^{\frac{p-1}{2}} \in \{\pm 1\}$.
2. En déduire que le symbole de Legendre

$$\left(\frac{\cdot}{p}\right) ; (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times, \quad a \mapsto a^{\frac{p-1}{2}},$$

   vu dans $\mathbb{C}$, est un caractère d'ordre exactement 2 de $(\mathbb{Z}/p\mathbb{Z})^\times$.
3. En déduire que a est un carré dans $(\mathbb{Z}/p\mathbb{Z})^\times$ si et seulement si $a^{\frac{p-1}{2}} = 1$. En déduire qu'un produit de deux non carrés est un carré.

TD n°5 : Actions de groupe et groupe symétrique

Exercice 1.

Soit G un groupe agissant sur un ensemble X. On se fixe un élément $x \in X$.

1. Montrer que $g_1 \bullet x = g_2 \bullet x$ ssi $\exists h \in \mathrm{Stab}_x$ tel que $g_1 = g_2 h$.
2. Rappeler pourquoi le stabilisateur de x est un sous-groupe de G.
3. En déduire que l'application
$$G \to X, \ \ g \mapsto g \bullet x$$
se factorise et corestreint en une bijection
$$G/\mathrm{Stab}_x \to \mathrm{Orb}_x$$
où l'ensemble source est celui des classes à gauches.

Exercice 2.

Soit G un groupe fini d'ordre pair. Nous voulons ici démontrer que G possède un élément d'ordre 2 (cela s'appelle le théorème de Cauchy pour un premier général). Nous détaillons la preuve pas à pas.

1. Démontrer que $g \mapsto g^{-1}$ est une bijection de G, d'ordre 2 vue dans le groupe des permutations $\mathfrak{S}_G$.
2. Démontrer que les points fixes de $g \mapsto g^{-1}$ sont précisément les éléments d'ordre divisant 2.
3. En déduire un morphisme de groupes $\mathbb{Z}/2\mathbb{Z} \to \mathfrak{S}_G$ et donc une action de $\mathbb{Z}/2\mathbb{Z}$ sur l'ensemble G.
4. En utilisant la formule des classes démontrer que G possède un nombre pair d'éléments d'ordre divisant 2.
5. Se rappeler l'existence du neutre et conclure que G possède un élément d'ordre 2.

Exercice 3.

Exhiber un élément d'ordre 6 dans $\mathfrak{S}_6$.

Exercice 4.

Soit $n \geq 2$ et $c = (1\,2\,\ldots\,n)$ un grand cycle fixé de $\mathfrak{S}_n$. Nous cherchons à déterminer son commutant.

1. Rappeler pourquoi $\langle c \rangle$ est contenu dans son commutant.
2. Soit σ dans son commutant. Démontrer que $\sigma c \sigma^{-1} = c$, puis que $(\sigma(1)\,\sigma(2)\,\ldots\,\sigma(n)) = (1\,2\,\ldots\,n)$.
3. Fixons i tel que $\sigma(1+i) = 1$. En déduire par récurrence sur j que pour tout j, nous avons $\sigma(j+i) = j$. Conclure que $\sigma = c^{\circ(-i)}$.

Exercice 5.

Soit G un groupe. Son groupe dérivé $\mathrm{D}(G)$ est le sous-groupe engendré par les commutateurs $[g:h] = ghg^{-1}h^{-1}$.

1. Démontrer que l'ensemble des commutatns de G est stable par conjugaison. En déduire que $\mathrm{D}(G)$ est stable par G.

   Indication : on pourra utiliser que le sous-groupe engendré par une partie et l'intersection des sous-groupes contenant cette partie, et en déduire que si la partie est stable par conjugaison, le sous-groupe aussi.
2. Démontrer que le quotient ${}^{G}/_{\mathrm{D}(G)}$ est abélien.
3. Soit $f : G \to A$ un morphisme de groupes vers un groupe abélien. Démontrer que $\mathrm{D}(G) \subseteq \mathrm{Ker}(f)$.

TD n°6 : Produits semi-directs

Exercice 1.

Soient N et K deux groupes. Soit $\alpha : K \to \mathrm{Aut}(N)$ un morphisme de groupes.

1. Vérifier que l'ensemble $N \times K$ muni de la loi $\star$ donnée par
$$\forall n, n' \in N, \forall k, k' \in K, \ \ (n,k) \star (n',k') = (n\alpha(k)(n'), kk')$$
est un groupe. Nous le notons $N \rtimes_\alpha K$.
2. Soit φ un automorphisme de K. Démontrer que l'application
$$N \rtimes_{\alpha\circ\varphi} K \to N \rtimes_\alpha K, \ \ (n,k) \mapsto (n, \varphi(k))$$
est un isomorphisme de groupes.

Exercice 2.

Nous considérons le sous-groupe $\mathrm{K}_4 = \{\mathrm{Id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ de $\mathfrak{A}_4$.

1. Vérifier que K_4 est bien un sous-groupe, puis en considérant le type cyclique de ses éléments, démontrer qu'il est distingué.
2. Démontrer qu'il existe une suite exacte courte
$$1 \to \mathrm{K}_4 \xrightarrow{\iota} \mathfrak{A}_4 \to \mathbb{Z}/3\mathbb{Z} \to 1.$$
3. Vérifier que $\langle (1\,2\,3) \rangle$ est un complément de K_4 dans $\mathfrak{A}_4$ et calculer l'automorphisme de K_4 qu'induit la conjugaison par $(1\,2\,3)$.
4. Démontrer que le morphisme
$$\left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\right) \rtimes_\alpha \mathbb{Z}/3\mathbb{Z} \to \mathfrak{A}_4, \ \ (a,b,c) \mapsto ((1\,2)(3\,4))^a((1\,3)(2\,4))^b(1\,2\,3)^c$$
est un isomorphisme, où α est défini tel que $\alpha(1)$ est l'automorphisme de $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ correspondant à la matrice $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$.

Exercice 3.

Considérons G le groupe des isométries de $\mathbb{Z}$, i.e. le groupe des bijections f de $\mathbb{Z}$ telles que $\forall (i,j) \in \mathbb{Z}^2,\ |f(i) - f(j)| = |i - j|$.

1. Soit N le groupe des translations défini par $N = \{i \mapsto i + n \,|\, n \in \mathbb{Z}\}$. Soit également $s = (i \mapsto -i)$ la symétrie par rapport à l'origine. Démontrer que s est d'ordre 2, que N et $\langle s \rangle$ sont des sous-groupes de G.
2. Démontrer que tout élément de G est une translation, ou la composée d'un translation et de s. En déduire que G est produit semi-direct interne de $\langle s \rangle$ par N. On vérifiera que la conjugaison par s stabilise N et envoie la translation par n sur la translation par $-n$.

TD n°7 : Symétries et groupe orthogonal

À venir l'année prochaine pour cause de séminaire.

TD n°8 : Géométrie (projective ?)

À venir l'année prochaine pour cause de canasson.

TD n°9 : Structure des groupes finis

Exercice 1.

1. Soit G un groupe d'ordre 60, quelles sont les valeurs possibles pour $\mathrm{n}_5(G)$? Donner un exemple de groupe G qui réalise chaque valeur prédite.
2. Soit G un groupe d'ordre pm avec $p \nmid m$. Soient g_1, g_2 deux éléments d'ordre p. Démontrer qu'il existe $g \in G$ et $i \in (\mathbb{Z}/p\mathbb{Z})^\times$ tels que $g_2 = g g_1^i g^{-1}$.
3. Soit G un groupe d'ordre $p^2 m$ avec $p \nmid m$. Soit $g \in G$ d'ordre p^2. Montrer que l'on se trouve exactement dans l'une des deux situations suivantes : il existe $g' \in G$ d'ordre p^2 tel que $g'^p = g$ ou il existe $g_1, g_2 \in G$ d'ordre p tels que $g_1 g_2 = g$ et $\langle g_1 \rangle \cap \langle g_2 \rangle = \{1\}$.
   Indication : *on pourra commencer par le cas d'un groupe d'ordre p^2.*

Exercice 2.

Soit $p < q$ deux premiers. Soit G un groupe d'ordre pq.

1. Utiliser le marteau de Sylow pour démontrer que G possède un sous-groupe distingué d'ordre q.
2. Utiliser le marteau de Schur-Zassenhaus pour démontrer que G est isomorphe à un produit semi-direct externe de $\mathbb{Z}/p\mathbb{Z}$ par μ_q.

Exercice 3.

Soit G un groupe et A un G-module. On rappelle qu'un 2-cocycle est une application $c : G \times G \to A$ telle que

$$\forall g, h, k \in G, \quad g \cdot c(h,k) - c(gh,k) + c(g,hk) - c(g,h) = 0.$$

1. Soit c un 2-cocycle tel que $c(1,1) = 0$. Vérifier que la formule

$$(a,g) \bullet (b,h) = (a + g \cdot b + c(g,h), gh)$$

définit une loi de groupe sur $A \times G$ telle que $A \times \{1\}$ est distingué. Appelons-la $A \times_c G$.

2. Construire une suite exacte

$$1 \to A \to A \times_c G \xrightarrow{\pi} G \to 1.$$

3. Soit H un sous-groupe de G. Démontrer que $c_H = c_{|H \times H}$ est encore un 2-cocycle et que $A \times_{c_H} H$ est isomorphe à $\pi^{-1}(H)$.
4. Vérifier que si la suite exacte pour $A \times_c G$ est scindée, elle l'est également pour $A \times_{c_H} H$. Le retrouver en considérant que la suite est scindée si et seulement si c (resp. c_H) est un 2-cobord.

Exercice 4.

Nous proposons une démonstration alternative de l'existence dans le théorème de Sylow : soit G un groupe fini et p un nombre premier tel que $|G| = p^n m$ avec $p \nmid m$, on veut prouver qu'il existe un sous-groupe de G d'ordre p^n.

1. Soit X l'ensemble des parties de G à p^n éléments. En considérant le polynôme $(1+x)^{p^n m}$ modulo p, démontrer que p ne divise pas $\binom{p^n m}{p^n} = |X|$.
2. En déduire qu'il existe une partie $H \in X$ telle que p ne divise pas $|\mathrm{Orb}(H)|$. En déduire que $p^n \mid |\mathrm{Stab}(H)|$
3. Soit $h \in H$. Démontrer que l'application

$$\mathrm{Stab}(H) \to H, \quad g \mapsto gh$$

est une injection. En déduire que $\mathrm{Stab}(H)$ est un p-Sylow de G.

TD n°10 : Annneaux

Exercice 1.

Soit A un anneau commutatif. Un élément $e \in A$ est dit idempotent si $e^2 = e$.

1. Soit e un élément idempotent. Démontrer que $e(1-e) = 0$.
2. En déduire que les idéaux Ae et $A(1-e)$ sont en somme directe puisque $A = Ae \oplus A(1-e)$.
3. À l'inverse, on suppose que $A = I \oplus J$ où I et J sont deux idéaux tels que $IJ = 0$. En décomposant 1 sur la somme directe, démontrer qu'il existe un idempotent $e \in I$.
4. Démontrer que $I = Ae$ et $J = A(1-e)$.

Exercice 2.

Un anneau A est dit noethérien si tout idéal de A est de type fini.
Soit A un anneau noethérien et $(I_n)_{n\in\mathbb{N}}$ une famille croissante d'idéaux.

1. Démontrer que $I = \cup_{n\in\mathbb{N}} I_n$ est un idéal de A.
2. En utilisant la noethérianité sur I, démontrer que $(I_n)_{n\geq 0}$ est constante pour n assez grand.

Réciproquement, soit A un anneau tel que toute suite croissante d'idéaux est constante à partir d'un certain rang. Soit I un idéal.

3. On construit par récurrence une famille d'idéaux comme suit. On pose $I_0 = (0)$. Puis, pour tout entier n, si $I_n = I$, on pose $I_{n+1} = I$, sinon on choisit $x_n \in I \backslash I_n$ et on pose $I_{n+1} = I_n + Ax_n$. Démontrer que (I_n) est une suite croissante d'idéaux de type fini contenus dans A.
4. Conclure que $I = I_n$ pour un certain $n \geq 0$ puis que I est de type fini.

Exercice 3.

Soit A un anneau. Démontrer qu'un élément premier est irréductible.

Exercice 4.

Soit A un anneau dans lequel tout idéal $aA + bA$ est principal [3].

1. Démontrer que si $aA + bA = dA$ alors d est un PGCD de a et b.
2. Démontrer que [4] $\mathrm{PGCD}(ab, ac) = a\,\mathrm{PGCD}(b, c)$
3. Démontrer que pour tout pgcd d de a et b

$$\mathrm{PGCD}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

3. On dit qu'un tel anneau est de Bézout
4. Ici les PGCD sont une classe d'équivalence pour la relation d'association.

TD n°11 : Modules

Exercice 1.

Soit $(G, +)$ un groupe abélien. Vérifier que l'élément 0, la loi $+$ et la loi

$$\times : \mathbb{Z} \times G \to G, \ \ (n, g) \mapsto ng$$

munissent G d'une structure de $\mathbb{Z}$-module. Démontrer que toute loi $\bullet$ telle que $(G, 0, +, \bullet)$ est une structure de $\mathbb{Z}$-module est en réalité la loi $\times$.

Exercice 2.

Soit A un anneau commutatif et $f : M \to N$ un morphisme A-linéaire entre A-modules.

1. Soit $m \in M$. Démontrer que $I_m = \{a \in A \,|\, am = 0\}$ est un idéal de A.
2. Démontrer que $I_m \subseteq I_{f(m)}$.

Nous appelons $\mathrm{Ann}(M) = \cap_{m \in M} I_m$ l'annulateur de M.

1. Démontrer que $\mathrm{Ann}(M)$ est un idéal de A.
2. Soit $m \in M$. Démontrer que l'application

   $$A \to M, \ \ a \mapsto am$$

   est un morphisme de groupes de noyau contenant $\mathrm{Ann}(M)$. En déduire qu'elle se factorise uniquement en une application

   $$A/\mathrm{Ann}(M) \to M.$$

3. En déduire qu'il existe une unique structure de $A/\mathrm{Ann}(M)$-module sur M telle que la loi externe $A \times M \to M$ se factorise par la nouvelle loi.

Exercice 3.

Soit A un anneau commutatif principal.

1. Démontrer qu'un A-module de type fini sans torsion (i.e. $\forall a \in A, m \in M, \ am = 0 \implies (a = 0 \text{ ou } m = 0)$) est libre.
2. Soit p un élément irréductible de A. Soit $d \geq 0$ et M un sous-A-module de $(A/(p))^d$. Démontrer que les facteurs invariants de M sont associés à 1 ou à p. En déduire que M est isomorphe à $(A/(p))^r$ pour un unique $0 \leq r \leq d$.