Gutsche Patrick

DM13

1) * Soit $x \in G$. $x + x = x - x = 0_G \in H$ donc R_H réflexive
* Soit $x, y \in G$ tq $x R y$. On a donc $y - x \in H$ or H est stable par passage à l'inverse donc $x - y \in H$, donc R_H symétrique.
* Soit $x, y, z \in G$ tq $x R y$ et $y R z$. Ainsi $y - x \in H$ et $z - y \in H$ or H est un sous-groupe donc $z - y + y - x = z - x \in H$ donc R_H transitive

Donc R_H est une relation d'équivalence

* Soient $x, y \in G$. $y \in \bar{x} \Leftrightarrow (\exists\, h \in H, y - x = h) \Leftrightarrow (\exists h \in H, y = x + h)$
donc $\bar{x} = x + H$.

2) * $\bar{x} + \bar{y} \triangleq \overline{x+y}$ a un sens si et seulement si $\overline{x+y}$ est bien une fonction de $\bar{x}$ et $\bar{y}$.
Il faut donc montrer que si $(\bar{x}, \bar{y}) = (\bar{a}, \bar{b})$, alors $\overline{x+y} = \overline{a+b}$.
Supposons donc que $\bar{x} = \bar{a}$ et $\bar{y} = \bar{b}$, où $x, y, a, b \in G$.
Alors $(x+y) - (a+b) = (x-a) + (y-b)$ or $x - a \in H$ car $x R_H a$ et $y - b \in H$. H étant un sous groupe, $(x+y) - (a+b) \in H$, donc $\overline{x+y} = \overline{a+b}$
* On montre facilement que + est associative et commutative : Soit $x, y, z \in H$.
$\bar{x} + \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} + \bar{x}$ et $(\bar{x} + \bar{y}) + \bar{z} = \overline{x+y} + \bar{z} = \overline{x+y+z}$
$= \bar{x} + \overline{y+z} = \bar{x} + (\bar{y} + \bar{z})$
* $\overline{0_G}$ est l'élément neutre : $\bar{x} + \bar{0} = \overline{x+0} = \bar{x} = \overline{0+x} = \bar{0} + \bar{x}$.
et pour tout $x \in H$, $-\bar{x} = \bar{0} - \bar{x} = \overline{-x}$.

* On procède par récurrence : Soit $a \in G$ et $n \in \mathbb{N}$, $R(n)$: $n\bar{a} = \overline{na}$
à $n = 0$: $0\bar{a} = \bar{0}$
à $n \geq 0$: $R(n)$: $n\bar{a} = \overline{na}$ donc $n\bar{a} + \bar{a} = \overline{na} + \bar{a} = (n+1)\bar{a} = \overline{(n+1)a}$
De plus $-n\bar{a} = -\overline{na} = \overline{-na}$

* Les sous-groupes de $\mathbb{Z}$ sont exactement les $n\mathbb{Z}$ avec $n \in \mathbb{N}$

$\mathbb{Z}/n\mathbb{Z} = \{\bar{k} \mid k \in \mathbb{Z}\} = \{k\bar{1} \mid k \in \mathbb{Z}\} = Gr(\bar{1})$ donc $\mathbb{Z}/n\mathbb{Z}$ monogène

* $k\bar{1} = 0 \iff \bar{k} = \bar{0} \iff k \in n\mathbb{Z}$, donc $\mathbb{Z}/n\mathbb{Z}$ est cyclique de cardinal n.

Donc $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$.

3) R_H est une relation d'équivalence donc elle partitionne G
donc $|G| = \sum_{C \in G/H} |C|$.

Soit $C \in G/H$. Il existe $x \in G$ tq $C = \bar{x} = x + H$.

Soit $\varphi : \begin{array}{l} H \longrightarrow x+H \\ h \longrightarrow x+h \end{array}$ est surjective par définition de $x+H$.

Si $\varphi(h) = \varphi(h')$, alors $x+h = x+h'$ donc $h = h'$ en composant $-x$.

donc φ bijective donc $|C| = |x+H| = |H|$

Donc $|G| = \sum_{C \in G/H} |C| = |H| \times |G/H|$.

4) G de type fini, donc on dispose de $n \in \mathbb{N}^*$ et de $(g_1, \dots, g_n) \in G^n$
tq $G = Gr(\{g_1, \dots, g_n\}) = \left\{ \sum_{i=1}^{n} \alpha_i g_i \mid (\alpha_i, \dots, \alpha_n) \in \mathbb{N}^n \right\}$.

De même, H étant de type fini, on dispose de $m \in \mathbb{N}^*$ et
de $(h_1, \dots, h_m) \in H^m$ tq $H = Gr(\{h_1, \dots, h_m\}) = \left\{ \sum_{i=1}^{n} \beta_i h_i \mid (\beta_1, \dots, \beta_n) \in \mathbb{N}^n \right\}$

Montrons que $G \times H = Gr(\{(g_1, 0), (g_2, 0), \dots, (g_n, 0), (0, h_1), \dots (0, h_m)\})$
ce qui permettra de conclure que $G \times H$ est de type fini.

$\boxed{\subset}$ Soit $z \in G \times H$. z s'écrit alors $z = (g, h)$ pour certains $g \in G$ et $h \in H$.
Comme $g \in G$, il existe $(\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ tq $g = \sum_{i=1}^{n} \alpha_i g_i$
Comme $h \in H$, il existe $(\beta_1, \dots, \beta_n) \in \mathbb{N}^m$ tq $h = \sum_{i=1}^{n} \beta_i h_i$
Alors $z = \left(\sum_{i=1}^{n} \alpha_i g_i, \sum_{i=1}^{n} \beta_i h_i \right) = \sum_{i=1}^{n} \alpha_i (g_i, 0) + \sum_{i=1}^{n} \beta_i (0, h_i)$
D'où $z \in Gr(\{(g_1, 0), \dots (g_n, 0), (0, h_1), \dots, (0, h_m)\})$.

$\boxed{\supset}$ Soit $z \in Gr(\{(g_1, 0), \dots, (g_n, 0), (0, h_1), \dots (0, h_m)\})$,
Il existe alors $(\alpha_1, \dots, \alpha_{n+m}) \in \mathbb{N}^{n+m}$ tq
$z = \alpha_1 (g_1, 0) + \alpha_2 (g_2, 0) + \dots + \alpha_n (g_n, 0) + \alpha_{n+1} (0, h_1) + \dots + \alpha_{n+m} (0, h_m)$

Donc $z = \Big(\underbrace{\sum_{i=1}^{n} \alpha_i g_i}_{\in G}, \underbrace{\sum_{i=1}^{m} \alpha_{n+i} h_i}_{\in H} \Big)$. D'où $z \in G \times H$.

On en déduit que $G \times H = Gr(\{(g_1,0),\dots,(g_n,0),(0,h_1),\dots,(0,h_m)\})$ et que $G \times H$ est donc de type fini.

5) Soit $a \in \mathbb{Z}$ tq $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}^*$. $n\bar{a} = \overline{na} = \bar{0}$ donc $\mathbb{Z}/n\mathbb{Z}$ de torsion

* Soit $a \in \mathbb{Z}^*$. Soit $n \in \mathbb{N}$ tq $na = 0$. alors $n = 0$ donc $\mathbb{Z}$ sans torsion.
* $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$: $(1,0)$ ordre ∞ car $n(1,\bar{0}) = (n,\bar{0})$
  $(0,1)$ ordre fini car $n(0,\bar{1}) = (0,\bar{0})$. Dc $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ n'est aucun des 2.
* $\mathbb{C}^*$: $(\mathbb{C}^*, \times)$ car $(\mathbb{C}^*, +)$ n'est pas un groupe. $(-1)^2 = 1$ donc -1 d'ordre fini (2)
  $2^n = 1 \Leftrightarrow n = 0$ donc 2 ordre infini. Dc $\mathbb{C}^*$ n'est aucun.
* Soit $x \in \mathbb{Q}/\mathbb{Z}$. On dispose de $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$ tq $x = \overline{\tfrac{a}{b}}$
  $bx = \bar{a} \underset{a \in \mathbb{Z}}{=} \bar{0}$

6) Supposons G est de cardinal fini. $G = Gr(G)$ or G fini donc G est de type fini.
Soit $a \in G$. On sait que $|G|a = 0$ donc $o(a) \leq |G|$ donc $o(a)$ finie donc G de torsion.

Supposons que G est de type fini et de torsion.
On dispose donc de $(g_1,\dots,g_m) \in G^m$ tq $G = Gr(\{g_1,\dots,g_m\})$
$= \{ \sum_{i=1}^{m} \alpha_i g_i \,/\, (\alpha_1,\dots,\alpha_m) \in \mathbb{N}^m \}$
or G est de torsion donc $g_1,\dots,g_m$ sont respectivement d'ordres $\gamma_1,\dots,\gamma_m$ finis
Donc $G = \{ \sum_{i=1}^{m} \alpha_i g_i \,/\, (\alpha_1,\dots,\alpha_m) \in [\![0,\gamma_1-1]\!] \times [\![0,\gamma_2-1]\!] \times \dots \times [\![0,\gamma_m-1]\!] \}$
car pour $i \in [\![1,n]\!]$ et $\alpha_i = q\gamma_i + r$ avec $0 \leq r \leq \gamma_i - 1$
$\alpha_i g_i = (q\gamma_i + r) g_i = q(\underbrace{\gamma_i g_i}_{0}) + r g_i = r g_i$

7) Soient $x, y \in G$ tq $o(x) \wedge o(y) = 1$.
$o(x)o(y)(x+y) = o(x)o(y)x + o(x)o(y)y$
$= o(y)\underbrace{o(x)x}_{0_G} + o(x)\underbrace{o(y)y}_{0_G} = 0_G$

* De même, $o(x+y)(x+y) = 0_G$ $\quad o(x)\,o(x+y)(x+y) = 0_G$

donc $o(x)o(x+y)y = 0_G$ donc $o(y) \mid o(x)\,o(x+y)$ car

$\alpha y = 0_G \Leftrightarrow \alpha = q\,o(y) + r$ avec $r \in [\![0, o(y)-1]\!]$ donc $ry = 0_G$ avec $r < o(y)$

i.e. $o(y) \mid \alpha$.

Or $o(y) \wedge o(x) = 1$ donc $o(y) \mid o(x+y)$.

De même, $o(x) \mid o(x+y)$. Or $o(x) \wedge o(y) = 1$ donc $o(x)o(y) \mid o(x+y)$

or $o(x+y) \neq 0$ donc $o(x)o(y) \leq o(x+y)$.

8) Soit $x, y \in G$. $x^{o(x)} = 1$ et $y^{o(y)} = 1$.

$\mathrm{ppcm}(o(x), o(y)) = p_1^{\alpha_1} p_2^{\alpha_2} \times \dots \times p_r^{\alpha_r}$ avec $(p_1, \dots, p_r) \in \mathbb{P}$ et $(\alpha_1, \dots, \alpha_r) \in \mathbb{N}$

donc soit $p_i^{\alpha_i} \mid o(x)$, soit $p_i^{\alpha_i} \mid o(y)$ parce que $\alpha_i = \max(v_{p_i}(o(x)), v_{p_i}(o(y)))$

SPDG, $p_i^{\alpha_i} \mid o(x)$.

$\frac{o(x)}{p_i^{\alpha_i}} x$ est d'ordre $p_i^{\alpha_i}$

De même, $\forall i \in [\![1, r]\!], \exists g_i \in G$ tq $o(g_i) = p_i^{\alpha_i}$.

D'après 7), $o(g_1 + \dots + g_r) = p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r} = \mathrm{ppcm}(o(x), o(y))$

9) $\forall x \in G, x^{|G|} = 1_G$ donc $\forall x \in G, o(x) \leq |G|$

donc l'ensemble des ordres $\{o(x) / x \in G\}$

est une partie de $\mathbb{N}$ majorée par $|G|$ donc

elle possède un maximum noté y.

Il existe donc $x_0 \in G$ tq $o(x_0) = y$.

Soit $x \in G$. D'après q8), il existe $z \in G$ tq

(1) $o(z) = o(x) \vee o(x_0)$. Or $o(x_0)$ est l'ordre maximal

donc $o(z) \leq o(x_0)$. De plus, cette équation implique que

$o(z) \geq o(x_0)$ car on a un ppcm. Donc $o(z) = o(x_0)$

Donc d'après (1), $o(x) \mid o(z) = o(x_0)$.

10) d'après 8), G est donc isomorphe à $H \times G/H$ où H est engendré par un élément d'ordre maximal x_0.
Dans cette question, nous noterons "$\equiv$" "isomorphe à".

$H = Gr(x_0)$ donc $H \equiv \mathbb{Z}/o(x_0)\mathbb{Z} = \mathbb{Z}/d_1\mathbb{Z}$ en notant $d_1 = o(x_0)$.

Donc $G \equiv \mathbb{Z}/d_1\mathbb{Z} \times G/H$

or d'après 2), G/H est un groupe abélien. De plus G/H est fini car G est fini. Donc d'après 8) puis 10), G/H est isomorphe à $H_2 \times (G/H)/H_2$ avec H_2 le groupe engendré par un ~~elément~~ élément d'ordre maximal de G/H.

Or d'après 8, l'ordre de tout $x \in G$ divise l'ordre de x_0, donc $H_2 \equiv \mathbb{Z}/d_2\mathbb{Z}$ avec $d_2 | d_1$.

$\rightarrow$ Donc $G \equiv \mathbb{Z}/d_1\mathbb{Z} \times H_2 \times (G/H)/H_2$

$\equiv \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times (G/H)/H_2$

$\rightarrow$ On en fait une récurrence.

D'après le théorème de Lagrange, $\#G = \#(G/H) \times \#H$

Pour un rang i, si $x_i \neq 0_{G/H/\dots}$ alors $\# H \geq 2$ car il contient $0_{G/H/\dots}$ et x_i car engendré par x_i.

Sinon, $G/H_1/H_2/\dots/H_i$ ne contient qu'un élément, donc il est isomorphe à $\mathbb{Z}/1\mathbb{Z}$ et on stoppe la récurrence, et

1 divise bien $d_{i}-1$.
Donc $(\#(G/H_{\ldots}))$ est strictement décroissante donc la récurrence est finie.

→ Donc il existe $l \in \mathbb{N}^*$ et $d_1, \ldots, d_l \in \mathbb{N}^*$ tels que
- pour tout $i \in \{1, \ldots, l-1\}$ $d_{i+1} | d_i$
- G isomorphe à $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_l\mathbb{Z}$

11) Reflexivité : Soit $(K, f) \in A$.
$K \subset K$ et $f|_K = f$ Donc $(K, f) \leq (K, f)$
Antisymmétrie : Soit $(K, f), (K', f') \in A$. Supposons $(K, f) \leq (K', f')$ et $(K', f') \leq (K, f)$.
Alors $K \subset K'$ et $f'|_K = f$ et $K' \subset K$ et $f|_{K'} = f'$
Donc $K = K'$ donc $f' = f$ Donc $(K, f) = (K', f')$
Transitivité : Soit $(K_1, f_1), (K_2, f_2), (K_3, f_3) \in A$.
Supposons que $(K_1, f_1) \leq (K_2, f_2)$ et $(K_2, f_2) \leq (K_3, f_3)$.
Alors $K_1 \subset K_2$ et $f_2|_{K_1} = f_1$ et $K_2 \subset K_3$ et $f_3|_{K_2} = f_2$
Donc $K_1 \subset K_3$ donc $f_3|_{K_1} = f_3|_{K_2}|_{K_1} = f_2|_{K_1} = f_1$
→ Donc "$\leq$" est une relation d'ordre sur A.

Partie IV - Sommes directes

14) a) $H_1 = Gr((2,1)) = \left\{ \sum_{i=1}^{n} \varepsilon_i \times (2,1) \,/\, n \in \mathbb{N} \text{ et } \varepsilon_1, \dots \varepsilon_n \in \{-1,1\} \right\}$
$= \{(2a, a) / a \in \mathbb{Z}\}$
$= 2\mathbb{Z} \times \mathbb{Z}$

$H_2 = Gr((0,2)) = \{(0, 2a), a \in \mathbb{Z}\} = \{0\} \times 2\mathbb{Z}$

Soit $(a,b) \in H_1 + H_2$ $a \in \{0 + 2\mathbb{Z}\} = 2\mathbb{Z}$ donc $(a,b) = (2 \times \frac{a}{2}, b) + (0,0)$

or si b pair, on a aussi $(a,b) = (2 \times \frac{a}{2}, 0) + (0, 2 \times \frac{b}{2})$

Contre-exemple : $(2,2) = (2 \times 1, 2) + (0, 2 \times 0)$
et $(2,2) = (2 \times 1, 0) + (0, 2 \times 1)$ donc $H_1 + H_2$ n'est pas direct.

b) Soit $a, b \in \mathbb{N}$, $H_1 = a\mathbb{Z}$, $H_2 = b\mathbb{Z}$.
Si $a = b = 1$, alors si $x \in H_1 + H_2$, $x = x + 0$ ou $x \in 0 + x$ donc $a\mathbb{Z} + b\mathbb{Z}$ n'est pas direct.

15) a) * Soit $x \in Gr(H_1 \cup H_2)$ on a $x = \sum_{i=1}^{n} h_i$ avec $h_1, \dots, h_n \in H_1 \cup H_2$

donc $x = \sum_{i=1}^{n} h'_i$ avec $l \in \{1, \dots, n\}$ et $h'_1, \dots, h'_l \in H_1$ et $h'_{l+1}, \dots, h'_n \in H_2$

H_1 (et H_2) sont des groupes donc $h'_1 + \dots + h'_l \in H_1$ (et $h'_{l+1} + \dots + h'_n \in H_2$)
Notons $a = h'_1 + \dots + h'_l \in H_1$ et $b = h'_{l+1} + \dots + h'_n \in H_2$
Donc $x = a + b$ donc $x \in H_1 + H_2$, Donc $Gr(H_1 \cup H_2) \subset H_1 + H_2$
* Soit $x \in H_1 + H_2$. il existe $h_1 \in H_1$ et $h_2 \in H_2$ tel que $x = h_1 + h_2$
or $h_1, h_2 \in H_1 \cup H_2$ donc $x = h_1 + h_2 \in Gr(H_1 \cup H_2)$
Donc $H_1 + H_2 \subset Gr(H_1 \cup H_2)$
→ Donc $H_1 + H_2 = Gr(H_1 \cup H_2)$.

b) $H_1 \oplus H_2$ est une somme directe donc $\forall h \in H_1 \oplus H_2$, il existe un unique $(h_1, h_2) \in H_1 \times H_2$ tel que $h = h_1 + h_2$.
Soit $f : H_1 \oplus H_2 \to H_1 \times H_2$ cette fonction.
$h \mapsto (h_1, h_2)$

f injective car Si $(h_1,h_2)=(h'_1,h'_2)$, $h_1=h'_1$ et $h_2=h'_2$ donc
$h_1+h_2=h'_1+h'_2$

f surjective : Soit $(h_1,h_2)\in H_1\times H_2$. $h_1+h_2\in H_1\oplus H_2$ par définition.

f est donc bijective.

Montrons que f est un morphisme : Soient $h,h'\in H_1\oplus H_2$. Il existe existe des uniques $(h_1,h_2),(h'_1,h'_2)\in H_1\times H_2$ tels que $h_1+h_2=h$ et $h'_1+h'_2=h'$

Donc $h+h'=h_1+h_2+h'_1+h'_2=(h_1+h'_1)+(h_2+h'_2)$ car $(G,+)$ commutatif

Donc $f(h+h')=(h_1,h'_2)+(h_1,h'_2)$ Donc f est un morphisme de groupes

→ Donc $H_1\oplus H_2$ et $H_1\times H_2$ isomorphes

16) * Soit $x\in(H_1+H_2)+H_3$. Il existe $(h,h_3)\in(H_1+H_2)\times H_3$ tels que $x=h+h_3$. Puis il existe $(h_1,h_2)\in H_1\times H_2$ tel que $h=h_1+h_2$

Donc $x=(h_1+h_2)+h_3$ or $(G,+)$ est associatif donc $x=h_1+(h_2+h_3)$ Donc $x\in H_1+(H_2+H_3)$. Donc $(H_1+H_2)+H_3\subset H_1+(H_2+H_3)$

* De même, $H_1+(H_2+H_3)\subset(H_1+H_2)+H_3$.

→ Donc $(H_1+H_2)+H_3=H_1+(H_2+H_3)$

* Supposons H_2+H_3 non directe. alors il existe $h\in H_2+H_3$ tel que il existe $(h_2,h_3),(h'_2,h'_3)\in H_2\times H_3$ différents tels que $h=h_2+h_3=h'_2+h'_3$.

Donc $(h_1+h_2)+h_3=(h_1+h'_2)+h'_3$ avec $h_1+h_2\neq h_1+h'_2$ ou $h_3\neq h'_3$

Donc $(H_1+H_2)+H_3$ ne serait pas direct. Contradiction,

→ Donc H_2+H_3 est une somme directe.

* Supposons $H_1+(H_2\oplus H_3)$ non directe. Alors il existe $(h_1,h_2,h_3)\in H_1\times H_2\times H_3$ et $(h'_1,h'_2,h'_3)\in H_1\times H_2\times H_3$ tels que $h_1\neq h'_1$ ou $h_2+h_3\neq h'_2+h'_3$ et tel que $h_1+(h_2+h_3)=h'_1+(h'_2+h'_3)$ ①

1e cas : $h_2+h_3=h'_2+h'_3$. Mais alors H_2+H_3 serait indirect, contradiction.

2e cas : $h_2+h_3\neq h'_2+h'_3$.

Si $h_1=h'_1$, ① montre que $h_2+h_3=h'_2+h'_3$, contradiction.

Si $h_1\neq h'_1$,

17) Soit $B=(x_i)_{i\in I}$ une base de G. Soit $x\in G\setminus\{0\}$. Par définition d'une base, il existe un unique $(n_i)\in \mathbb{Z}^{(I)}$ tel que $x=\sum_{i\in I} n_i x_i$
Supposons qu'il existe $y\in\mathbb{Z}$ tel que $yx=0_G$.
Donc $\sum_{i\in I} y n_i x_i = 0_G$. Or $\sum_{i\in I} 0 x_i = 0_G$ donc par unicité de (n_i),
$\forall i\in I, yn_i = 0_G$
Or $x\neq 0$ Donc il existe $i\in I$ tel que $n_i\neq 0$. Or $yn_i=0$ donc $y=0$
→ Donc G est sans torsion.

18) a) Soit $C=(e_i)_{i\in I}$ une autre base de G. Supposons C infini.
Pour tout $x\in(e_i)$, x s'écrit sous la forme d'une combinaison linéaire finie des éléments de (x_i). Donc il existe une famille $(n_{i,1}, n_{i,2},\dots)$ à support fini (i.e. tel que il existe $K_i\subset\mathbb{N}$ fini tel que $n_{i,k}\neq 0$ si et seulement si $k\in K_i$) tel que $x_i = \sum_{k=1}^{+\infty} n_{i,k} y_k$.

chaque $x\in G$ s'écrit sous la forme d'une combinaison linéaire finie des éléments de (e_i). Mais donc aussi en fonction des éléments de $C' = \bigcup_{i=1}^{n} \bigcup_{k\in K_i}\{e_k\}$, qui est un ensemble fini.

$C'\subset C$ et C' fini alors que C est infini. Donc il existe $z\in C$ tel que $z\notin C'$
En écrivant z à partir des éléments de B, puis en remplaçant les éléments de B par une combinaison linéaire des éléments de C', on obtient une écriture de z en fonction des éléments de C différente de $z=z$. Cela contredit la définition d'une base.

b)