Tous les résultats introduits par "On remarquera que..." peuvent être utilisés sans démonstration et ne doivent pas être démontrés.

Partie 1
Partitions d'un entier

On appelle partition d'un entier n une suite $\lambda = (r_k)_{k\geq 1}$ d'entiers naturels tels que $\sum_{k=1}^{+\infty} k r_k = n$. L'entier r_k s'appelle la multiplicité de k dans la partition λ.

Si $r_k \geq 1$ on dit que k est une part de la partition. Il existe une unique partition de 0, elle ne possède aucune part et se note 0. La partition $\lambda = (r_k)_{k\geq 1}$ de n se note formellement $(1^{r_1}\, 2^{r_2} \cdots)$. La taille de la partition $\lambda = (r_k)_{k\geq 1}$ est par définition l'entier $r = \sum_{k=1}^{+\infty} r_k$. Si λ n'est pas la partition 0, il sera pratique de noter ses parts dans l'ordre décroissant de leur valeur $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r > 0$. Pour une partition λ, on définira la suite $(\lambda_i)_{i\in\mathbf{N}^*}$ de ses parts en complétant la suite précédente par $\lambda_i = 0$ pour $i \geq r+1$.

Donnons un exemple : $(1, 0, 2, 0, 1, 0, \cdots)$ est une partition de $n = 12$ associée à la décomposition $12 = 5 + 3 + 3 + 1$. Elle se note $(1^1 2^0 3^2 4^0 5^1 \cdots)$ ou $(1^1\, 3^2\, 5^1)$. Elle est de taille $r = 4$ et on a $\lambda_1 = 5, \lambda_2 = \lambda_3 = 3, \lambda_4 = 1$.

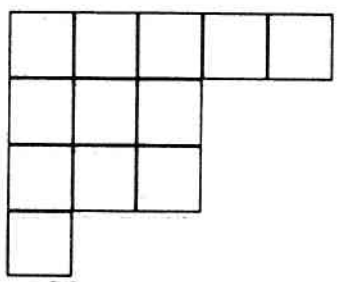
On constatera (sans avoir à en faire la preuve) que, réciproquement, la donnée d'une suite $(\lambda_i)_{i\in\mathbf{N}^*}$ telle qu'il existe un entier r vérifiant

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r > 0 \quad \text{et} \quad \lambda_i = 0 \text{ pour } i \geq r+1$$

détermine une unique partition λ de l'entier $n = \sum_{i=1}^{+\infty} \lambda_i$ dont la taille est r et dont la suite des parts est la suite donnée. L'entier n s'appelle alors le poids de la partition λ et se note $|\lambda|$.

On peut représenter λ par un diagramme de n carrés rangés en r lignes, la $i^{\text{ème}}$ ligne contenant exactement λ_i carrés.

Un exemple : la partition précédente est associée au diagramme :



Si l'on transpose le diagramme d'une partition $\lambda = (r_k)_{k\geq 1}$ de n par rapport à la diagonale (de telle sorte que la $i^{\text{ème}}$ colonne devienne la $i^{\text{ème}}$ ligne) on obtient un diagramme associé à une nouvelle partition $\lambda' = (r'_k)_{k\geq 1}$ de n, que l'on appelle la conjuguée de λ. Dans l'exemple on obtient la partition $12 = 4+3+3+1+1$. La taille de λ' sera notée r' et la suite de ses parts $(\lambda'_i)_{i\in\mathbb{N}^*}$.

1) Exprimer r' ainsi que les r'_k à l'aide des λ_i. En déduire l'expression des λ_i en fonction des r'_k, puis des λ'_i en fonction des r_k.

On remarquera que $\lambda'_j = \text{Card}\,\{i; \lambda_i \geq j\}$.

Si λ et μ sont deux partitions, dont les suites des parts sont respectivement $(\lambda_i)_{i\in\mathbb{N}^*}$ et $(\mu_i)_{i\in\mathbb{N}^*}$, on écrira $\lambda \subset \mu$ si et seulement si $\lambda_i \leq \mu_i$ pour tout entier i plus grand que 1.

2) Montrer que $(\lambda \subset \mu)$ si et seulement si $(\lambda' \subset \mu')$.

Définissons deux additions sur l'ensemble P des partitions par des opérations géométriques sur les diagrammes qui leur sont associés.

En additionnant à chaque ligne du diagramme associé à la partition λ de n la ligne correspondante du diagramme de la partition μ de m, nous obtenons une partition notée $\lambda + \mu$ de $n+m$. Une opération similaire sur les colonnes des diagrammes nous donne la partition $\lambda \oplus \mu$ de $n+m$.

3) Quel est le lien entre les opérateurs $+$, $\oplus$ et $'$?

Partie 2
Quelques lemmes

4) On se place dans l'algèbre $\mathbb{Q}[X,T]$ des polynômes à deux indéterminées sur le corps des rationnels.

   a) Montrer qu'il existe une famille de polynômes en une seule indéterminée à coefficients entiers positifs, notés $P_{n,k}(X)$, $0 \leq k \leq n$, telle que pour tout entier n :

$$\prod_{i=0}^{n-1}(1+X^iT) = \sum_{k=0}^{n} X^{\frac{k(k-1)}{2}} P_{n,k}(X)T^k \quad .$$

   On prendra pour convention $P_{0,0} = 1$.

   b) Déterminer la relation de récurrence définissant de manière unique la famille précédente.

5) On considère la famille de fractions rationnelles

$$F_{n,k}(X) = \frac{(1-X^{n-k+1})\cdots(1-X^n)}{(1-X)\cdots(1-X^k)},$$

pour $1 \leq k \leq n$ et $F_{n,0} = 1$, n et k entiers positifs.

a) Montrer que $F_{n,k}$ est en fait un polynôme à coefficients entiers positifs.

b) Quel est son degré ?

c) Prouver l'égalité de $F_{n,k}$ et $F_{n,n-k}$, pour tout couple (n,k) d'entiers vérifia $0 \leq k \leq n$.

6) Soit E un espace vectoriel de dimension n sur le corps $\frac{\mathbb{Z}}{p\mathbb{Z}}$, où p est un nombre premi

a) Exprimer à l'aide des polynômes précédents le nombre de sous-espaces de dime sion r de E.

b) Si F est un sous-espace de dimension l de E, exprimer de même le nomb $c_{n,l,r}$ de sous-espaces G tels que $F \subset G \subset E$ et $\dim G = r$. Justifier l relation $c_{n,l,r} = c_{n,l,n-r+l}$, où (n,l,r) est un triplet quelconque d'entiers vérifia $0 \leq l \leq r \leq n$.

c) Prouver que $\sum_{k=0}^{n-l} (-1)^k p^{\frac{k(k-1)}{2}} c_{n,l,l+k}$ vaut 1 si $n = l$ et 0 si $n > l$.

d) En déduire que si (f_F) et (g_F) sont deux suites de réels indexées par les sou espaces F de E telles que, pour tout sous-espace F de E, on ait

$$f_F = \sum_{G \subset F} g_G,$$

alors, pour tout sous-espace F de E,

$$g_F = \sum_{G \subset F} (-1)^l p^{\frac{l(l-1)}{2}} f_G,$$

où l (que l'on aurait dû noter $l_F(G)$), est la codimension de G dans F.

On s'intéresse maintenant aux groupes commutatifs. On notera leur loi $+$. On rappell que tout groupe commutatif est naturellement muni d'une structure de module sur $\mathbb{Z}$. S G est un groupe commutatif et n un entier la notation nG désigne l'ensemble $\{ng\,;\, g \in G\}$.

7) Soient H et K deux sous-groupes du groupe commutatif G.

a) Si $K \subset H \subset G$, démontrer que $\frac{H}{K}$ est un sous-groupe de $\frac{G}{K}$ et que $\frac{\frac{G}{K}}{\frac{H}{K}}$ est isomorphe à $\frac{G}{H}$.

b) Prouver que $\frac{H}{H \cap K}$ est isomorphe à $\frac{H+K}{K}$.

c) Soit q un entier positif, montrer que $\frac{qG}{H \cap qG}$ est isomorphe à $q\frac{G}{H}$, sous-groupe de $\frac{G}{H}$.

Partie 3
Les p-groupes commutatifs finis

Soit p un nombre premier. On considère un p-groupe G, commutatif et fini. On rappelle qu'il est isomorphe à

$$G_\lambda(p) = \frac{\mathbb{Z}}{p^{\lambda_1}\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{p^{\lambda_r}\mathbb{Z}}$$

avec $\lambda_1 \geq \cdots \geq \lambda_r > 0$, et $\lambda_1 + \cdots + \lambda_r = n$ avec $\operatorname{Card} G = p^n$. De plus, ces conditions déterminent la suite λ de manière unique, ce qui nous permet d'établir une bijection entre l'ensemble des classes d'isomorphisme de p-groupes commutatifs finis et l'ensemble des partitions.

Si G est un groupe isomorphe à $G_\lambda(p)$, on dira qu'il est de type λ. Si H est un sous-groupe de G tel que $\frac{G}{H}$ soit de type ν, on dira que H est de cotype ν dans G. Si G est de type λ, le poids de λ s'appelle la longueur de G ; on la note $l(G)$. Elle est aussi définie par $\operatorname{Card} G = p^{l(G)}$.

CONVENTION : *Dans la suite tous les groupes considérés sont des p-groupes commutatifs finis.*

8) On s'intéresse au comportement du type vis-à-vis des opérations sur les groupes.

   a) Exprimer le type du produit direct des groupes G et H en fonction des types de G et H.

   b) Montrer que $l(\frac{G}{H}) = l(G) - l(H)$ si H est un sous-groupe de G.

   c) Soient $K \subset H$ deux sous-groupes du groupe G. Montrer que le cotype de H dans G est égal au cotype de $\frac{H}{K}$ dans $\frac{G}{K}$.

Construisons une algèbre sur le corps des rationnels notée $A(p)$ de la manière suivante : comme base de l'espace vectoriel $A(p)$, nous choisissons les $G_\lambda(p)$ eux-mêmes, où λ parcourt l'ensemble Λ des partitions. Un élément de $A(p)$ est une somme $\sum_{\lambda\in\Lambda} a_\lambda G_\lambda(p)$ où les a_λ sont des rationnels, nuls sauf pour un nombre fini de λ. Nous définissons dans $A(p)$ la multiplication distributive par la règle

$$G_\lambda(p)G_\mu(p) = \sum_{\rho\in\Lambda} g^\rho_{\lambda\mu}(p) G_\rho(p),$$

où $g^\rho_{\lambda\mu}(p)$ est le nombre de sous-groupes H de $G_\rho(p)$ tels que

$$H \sim G_\lambda(p), \quad \frac{G_\rho(p)}{H} \sim G_\mu(p)$$

(c'est à dire le nombre de sous-groupes H de $G_\rho(p)$ de type λ et de cotype μ), la loi s'étendant à $A(p)$ par bilinéarité.

9) Montrer que $g^{\rho}_{\lambda\mu}(p) = 0$ sauf si $|\rho| = |\lambda| + |\mu|$. En déduire que la multiplication de $A(p)$ est bien définie.

On notera $g^{\rho}_{\lambda_0\lambda_1\cdots\lambda_k}(p)$ le nombre de chaînes de sous-groupes $H_1 \subset H_2 \subset \cdots \subset H_k$ dans $G_\rho(p)$, telles que $H_1, \dfrac{H_2}{H_1}, \ldots, \dfrac{G_\rho(p)}{H_k}$ soient respectivement de type $\lambda_0, \lambda_1, \ldots, \lambda_k$.

10) Justifier l'associativité de la multiplication de $A(p)$.

11) Soit G un p-groupe commutatif fini. On appelle dual de G, noté $\widehat{G}$, l'ensemble des homorphismes de groupes de G dans le groupe multiplicatif des nombres complexes. Cet ensemble $\widehat{G}$ est un groupe lorsqu'on le munit de la loi :

$$\forall(\phi,\psi) \in \widehat{G}^2 \quad \forall g \in G \quad \phi\psi(g) = \phi(g)\psi(g).$$

Soit H un sous-groupe de G. On pose $H^\circ = \{\phi \in \widehat{G}; \phi(H) = \{1\}\}$. Soit K un sous-groupe de $\widehat{G}$. On pose $K^\perp = \{x \in G; \forall \phi \in K \ \phi(x) = 1\}$.

a) Montrer que $\widehat{G}$ est isomorphe à G.

b) Montrer que pour x non nul dans G, il existe un élément ϕ de $\widehat{G}$ tel que $\phi(x) \neq 1$ (on pourra faire la démonstration dans le cas de $G_\lambda(p)$). En déduire que $\Phi : x \mapsto (\phi \mapsto \phi(x))$ est un isomorphisme de G sur $\widehat{\widehat{G}}$.

c) Montrer que H° est isomorphe à $\widehat{\left(\dfrac{G}{H}\right)}$.

d) Montrer que $\dfrac{\widehat{G}}{H^\circ}$ est isomorphe à $\widehat{H}$.

e) Prouver que l'application $H \mapsto H^\circ$ est une bijection de l'ensemble des sous-groupes de G sur l'ensemble des sous-groupes de $\widehat{G}$.

f) Déduire des questions précédentes que la multiplication de $A(p)$ est commutative.

12) Etablir que si G est un groupe de type λ et si pour tout entier i non nul on pose $\mu_i = l(\dfrac{p^{i-1}G}{p^iG})$, alors $\mu = \lambda'$.

13) Prouver que si G est un groupe de type ρ, H un sous-groupe de G de type λ et de cotype μ, alors $\lambda \subset \rho$ et $\mu \subset \rho$ (on établira d'abord $\mu' \subset \rho'$).

Partie 4
Dénombrement de sous-groupes

On rappelle que p est un nombre premier et que tous les groupes considérés sont des p-groupes commutatifs finis. On dira qu'un groupe G est élémentaire si $pG = 0$.

14) Prouver que tout groupe G possède un plus grand sous-groupe élémentaire, que l'on appellera le socle de G, noté S. Exprimer le cotype $\tilde{\lambda}$ de S à l'aide du type λ de G.

15) Montrer que tout groupe élémentaire peut être naturellement muni d'une structure d'espace vectoriel sur le corps $\frac{\mathbb{Z}}{p\mathbb{Z}}$.

Soit H un sous-groupe de G tel que $\frac{G}{H}$ soit élémentaire. Par définition, une famille $(x_1, \ldots, x_l)$ d'éléments de G est libre modulo H si et seulement si la famille des images de ces éléments dans le $\frac{\mathbb{Z}}{p\mathbb{Z}}$-espace vectoriel $\frac{G}{H}$ est libre.

16) Soient G un groupe et H un sous-groupe de G tel que $\frac{G}{H}$ soit élémentaire. Calculer en fonction de l et des longueurs de G et H, le nombre de familles $(x_1, \ldots, x_l)$ d'éléments de G libres modulo H, dans le cas $0 \leq l \leq l(G) - l(H)$.

17) On se donne un groupe élémentaire G, deux sous-groupes H' et H de G et un entier l, avec $H' \subset H$ et $0 \leq l \leq l(G) - l(H)$. On voudrait dénombrer les sous-groupes G' de G tels que :

(C) $$G' \cap H = H' \quad , \quad l(\frac{G'}{H'}) = l \quad .$$

(On remarquera que les groupes $\frac{G}{H}$ et $\frac{G}{H'}$ sont élémentaires.)

a) Soit $(x_1, \ldots, x_l)$ une famille d'éléments d'éléments de G libre modulo H. Prouver que si G' est le sous-groupe engendré par H' et les éléments de cette famille, alors il vérifie la condition (C).

b) Montrer que tout sous-groupe G' vérifiant la condition (C) est engendré par H' et les éléments d'une famille $(x_1, \ldots, x_l)$, $x_i \in G$, libre modulo H.

c) Donner le nombre de sous-groupes G' de G vérifiant la condition (C), et en déduire que ce nombre est une fonction polynomiale de p.

Partie 5
Précisions sur $g^{\rho}_{\lambda\mu}(p)$

On se propose de démontrer que $g^{\rho}_{\lambda\mu}(p)$ est une fonction polynomiale de p.

18) Soient G un groupe de type ρ, H un sous-groupe de cotype α dans G, β une partition telle que $\alpha \subset \beta \subset \rho$. Posons $H_i = p^i G \cap H$.

a) Montrer $l(H_i) = \sum_{j>i} (\rho'_j - \alpha'_j)$, en prouvant auparavant que

$$l(H_i) = l(p^i G) - l(p^i \frac{G}{H}) \quad .$$

b) Soit K un sous-groupe de H ; notons $K_i = K \cap p^i G = K \cap H_i$. Prouver que K est de cotype β dans G si et seulement si pour tout entier i non nul $l(K_{i-1}) - l(K_i) = \rho'_i - \beta'_i$.

c) On suppose de plus que H est élémentaire. Montrer que le nombre de sous-groupes K de G, contenus dans H et de cotype β dans G, est une fonction polynomiale de p, notée $h_{\alpha\beta\rho}(p)$.

19) Soient G un groupe de type ρ, H un sous-groupe de G ; pour tout sous-groupe L de H, on désigne par $f(H,L)$ (resp. $g(H,L)$) le nombre de sous-groupes K de cotype α dans G tels que $pK \subset L \subset H \subset K$ (resp. $pK = L \subset H \subset K$). Etablir :

$$f(H,L) = \sum_{T \subset L} g(H,T),$$

en déduire

$$g(H,L) = \sum_{T \subset L} (-1)^m p^{\frac{m(m-1)}{2}} f(H,T),$$

où $m = l(\frac{L}{T})$.

20) Soit G un groupe de type ρ, H un sous-groupe élémentaire de cotype β dans G, L un sous-groupe de H de cotype γ dans G. Nous aurons $\alpha \subset \beta \subset \gamma \subset \rho$.

a) Montrer qu'il existe un sous-groupe S de G contenant H tel que $\frac{S}{L}$ soit le socle de $\frac{G}{L}$.

b) Soit K un sous-groupe de G contenant H, de cotype α dans G ; montrer que $pK \subset L \subset H \subset K$ si et seulement si $\frac{K}{H} \subset \frac{S}{H}$. En déduire l'égalité $f(H,L) = h_{\tilde{\gamma}\alpha\beta}(p)$.

c) Prouver qu'il existe un polynôme $F_{\alpha\beta\rho}(X)$ à coefficients entiers tel que le nombre de sous-groupes K de cotype α dans G tels que $pK = H$ soit égal à $F_{\alpha\beta\rho}(p)$.

Soit G un groupe de type ρ, soit H un sous-groupe de type λ et de cotype μ. Pour tout i, soit $\rho^{(i)}$ le cotype de $p^i H$. Soit r le plus petit entier tel que $p^r H = \{0\}$. On note $U(H)$ la suite $(\rho^{(0)}, \ldots, \rho^{(r)})$. On remarquera que $\rho^{(0)} = \mu$ et $\rho^{(r)} = \rho$. Toute suite de partitions pouvant s'obtenir par ce procédé (choix d'un entier premier p, puis d'un p-groupe commutatif G et d'un de ses sous-groupes H et construction de la suite des cotypes) s'appellera une RL-suite.

On admettra que la propriété pour une suite $(\rho^{(0)}, \ldots, \rho^{(r)})$ d'être une RL-suite est indépendante de p : si $(\rho^{(0)}, \ldots, \rho^{(r)})$ est une RL-suite pour un entier premier p, elle l'est pour tout autre entier premier.

21) Prouver que l'ensemble des RL-suites $(\rho^{(0)}, \ldots, \rho^{(r)})$ telles que $\rho^{(0)} = \mu$ et $\rho^{(r)} = \rho$ est fini.

22) Soient G un groupe de type ρ et

$$U = (\rho^{(0)} = \mu, \ldots, \rho^{(r)} = \rho)$$

une RL-suite. On note $g_U(p)$ le nombre de sous-groupes H de G de type λ et de cotype μ tels que $U(H) = U$.

a) Montrer que si chaque $g_U(p)$ est une fonction polynomiale de p, il en est de même de $g^{\rho}_{\lambda\mu}(p)$.

b) Soit H un sous-groupe tel que $U(H) = (\rho^{(0)}, \ldots, \rho^{(r)})$, notons $H' = pH$. Prouver que $U(H') = (\rho^{(1)}, \ldots, \rho^{(r)}) = U'$.

c) Soit H' un sous-groupe de G tel que $U(H') = U'$. Alors le nombre de sous-groupes H de G tels que $U(H) = U$ et $pH = H'$ est $F_{\rho^{(0)}\rho^{(1)}\rho^{(2)}}(p)$ (indication : quotienter par pH'). En déduire $g_U(p) = F_{\rho^{(0)}\rho^{(1)}\rho^{(2)}}(p) g_{U'}(p)$.

d) En déduire que $g_U(p)$ est une fonction polynomiale. Il en est donc ainsi de $g^{\rho}_{\lambda\mu}(p)$.