Je tiens à remercier Monsieur Abdelmejid BAYAD qui, grâce à ses nombreuses suggestions et critiques, m'a permis de mener à bien la réalisation de ce Travail d'Etude et de Recherche.

Table des matières

Chapitre 1

INTRODUCTION.

La fonction factorielle apparaît dans nombre de situations mathématiques.Citons les coefficients binômiaux, la formule de Stirling, la fonction Gamma et la fonction exponentielle.Il est en effet presque impossible d'étudier une question de combinatoire sans maîtriser les factorielles.
Le but de ce TER est tout d'abord de faire le point sur les applications arithmétiques de la fonction factorielle usuelle.On énonce plusieurs résultats d'arithmétique où la fonction factorielle joue un rôle central.Ensuite pour étendre, entre autres, ces résultats d'arithmétique aux sous-ensembles de $\mathbb{Z}$ et à des anneaux plus généraux que $\mathbb{Z}$, on développe une théorie permettant d'introduire des fonctions factorielles généralisées.
Ce TER se compose de deux parties : la première comporte une étude théorique de la fonction factorielle et sa généralisation, la seconde est réservée aux applications de la fonction factorielle généralisée.
Ces factorielles généralisées ont été introduites le plus souvent pour répondre à des questions déjà anciennes en théorie des nombres et en analyse complexe mais sont aujourd'hui utilisées pour de nouvelles questions dont certaines attendent encore des réponses en particulier les problèmes de combinatoire.
Ce TER a été réalisé à partir d'un article publié par MANJUL BHARGAVA dans "The mathematical association of America" en novembre 2000.
Nous nous sommes servis des pages 783 à 798.
Il est a noter que cet article comporte des erreurs auxquelles nous avons remédié (pages 54, 56 et 59).

Première partie

THEORIE.

Chapitre 2

LA FONCTION FACTORIELLE EN THEORIE DES NOMBRES.

Ce chapitre regroupe des résultats fondamentaux d'arithmétique dans lesquels la fonction factorielle joue un rôle prépondérant.

2.1 Factorielle et combinatoire.

L'exemple le plus connu des fonctions factorielles qui apparaît en théorie des nombres est probablement le résultat de divisibilité suivant :

Théorème 1 *Le produit de k entiers consécutifs est divisible par $k!$.*

Bien qu'admettant un énoncé trivial, ce résultat est plus important en théorie des nombres qu'il n'y paraît au premier abord.
Nous pouvons restituer ce résultat comme suit :

Théorème 2 *Soient $k, l \in \mathbb{N}$*
alors $(k+l)!$ est un multiple de $k! \times l!$.

Le théorème 2 est manifestement équivalent au théorème 1, et de plus , sa preuve est clairement combinatoire.

Preuve du théorème 2 :
Soient $k, l \in \mathbb{N}$,
on a :

$$\begin{pmatrix} l+k \\ l \end{pmatrix} = \frac{(l+k)!}{l! \times (l+k-l)!}$$

$$= \frac{(l+k)!}{l! \times k!}$$

puisque $\begin{pmatrix} l+k \\ l \end{pmatrix} \in \mathbb{N}$
alors $\frac{(l+k)!}{l! \times k!} \in \mathbb{N}$
donc $\forall\ l, k \in \mathbb{Z}$, $l! \times k!$ divise $(l+k)!$

•

2.2 Diviseur fixe de f sur $\mathbb{Z}$

Il y a cependant d'autres résultats des fonctions factorielles en théorie des nombres qui ne sont pas aussi triviaux.
Un exemple est dû à Georges POLYA qui décrit, en 1915, la relation proche entre les fonctions factorielles et les ensembles possibles de valeurs prises par un polynôme.

Définition 1 *Soit f un polynôme à coefficients entiers*
alors $d(\mathbb{Z}, f)$= pgcd $(f(a)$: $a \in \mathbb{Z})$
$d(\mathbb{Z}, f)$ est appelé le diviseur fixe de f sur $\mathbb{Z}$.

Par exemple, considérons le polynôme $f(x) = x^5 + x$
$*$ si x est pair,
$f(x)$ est la somme de 2 nombres pairs
donc $f(x)$ est pair.
$*$ si x est impair,
$f(x) = x \times (x^4 - 1)$ est le produit d'un nombre pair par un nombre impair
donc $f(x)$ est encore pair.
Il s'ensuit que $d(\mathbb{Z}, f)$ est multiple de deux.
D'autre part, $f(1) = 2$
d'où $d(\mathbb{Z}, f) = 2$.

$*$ Quelles sont les valeurs possibles de $d(\mathbb{Z}, f)$?
Prenons $g(x) = 1000x^5 + 1000x$ (ie $g(x) = 1000f(x)$)
alors $d(\mathbb{Z}, g) = 2000$
c'est à dire que si nous multiplions un polynôme f par $k \in \mathbb{Z}$ alors $d(\mathbb{Z}, f)$ est aussi multiplié par k.
Il suffit donc de trouver $d(\mathbb{Z}, f)$ pour les polynômes primitifs c'est à dire $f(x) = a_0 + a_1 x + ... + a_n x^n$ tel que $pgcd(a_0, ..., a_n) = 1$.
Dans ce cas, notre question a la réponse suivante :

Théorème 3 *Soit f un polynôme primitif de dégré k,*
alors $d(\mathbb{Z}, f)$ divise $k!$.

Remarque 1 *Non seulement $k!$ est une borne supérieure pour le diviseur fixe des polynômes de degré k sur $\mathbb{Z}$, mais $k!$ en fait peut être atteint pour un polynôme primitif f,*
c'est à dire $d(\mathbb{Z}, f) = k!$ pour un polynôme primitif de degré k.

Preuve de la remarque 1 :
Soit $P(x) = x \times (x-1) \times ..... \times (x-(k-1))$
alors $P(x)$ est le produit de k nombres consécutifs
donc $P(x)$ est multiple de $k!$ (d'après le théorème 1).
D'autre part,

$$\begin{aligned} P(k) &= k \times (k-1) \times ..... \times 1 \\ &= k! \end{aligned}$$

d'où $d(\mathbb{Z}, P) = k!$

•

Preuve du théorème 3 :
Soit $P(X) = a_0 + a_1X + ... + a_kX^k$, un polynôme primitif de degré k
donc tel que $pgcd(a_0, ..., a_k) = 1$.
Exprimons $P(X)$ dans la base $(1, X, X(X-1), X(X-1)(X-2), ...)$
$P(X)$ devient :
$P(X) = c_0 + c_1X + c_2X(X-1) + ... + c_kX(X-1)...(X-(k-1))$ polynôme primitif de degré k.
Calculons les premiers termes afin d'écrire $P(X)$ sous forme de matrice :
$P(0) = c_0$
$P(1) = c_0 + c_1$
$P(2) = c_0 + 2c_1 + 2c_2 = c_0 + 2c_1 + 2!c_2$
$P(3) = c_0 + 3c_1 + 6c_2 + 6c_3 = c_0 + 3c_1 + 6c_2 + 3!c_3$
$P(4) = c_0 + 4c_1 + 12c_2 + 24c_3 + 24c_4 = c_0 + 4c_1 + 12c_2 + 24c_3 + 4!c_4$
$P(5) = c_0 + 5c_1 + 20c_2 + 60c_3 + 120c_4 + 120c_5 = c_0 + 5c_1 + 20c_2 + 60c_3 + 120c_4 + 5!c_5$
.
.
.

$$\text{donc } \begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & \cdots\cdots & \cdots & \cdots & 0 \\ 1 & 1! & 0 & \cdots & \cdots & \cdots\cdots & \cdots & \cdots & 0 \\ 1 & 2 & 2! & 0 & \cdots & \cdots\cdots & \cdots & \cdots & 0 \\ 1 & 3 & 6 & 3! & 0 & \cdots & \cdots & \cdots & 0 \\ 1 & 4 & 12 & 24 & 4! & 0 & \cdots & \cdots & 0 \\ 1 & 5 & 20 & 60 & 120 & 5! & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & k & k(k-1) & k(k-1)(k-2) & \cdots & \cdots\cdots & \cdots & \cdots & k! \end{pmatrix} \times \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ \vdots \\ \vdots \end{pmatrix}$$

$$= \begin{pmatrix} P(0) \\ P(1) \\ P(2) \\ P(3) \\ P(4) \\ P(5) \\ \vdots \\ \vdots \end{pmatrix}$$

soit $M(k) \times C(k) = Q(k)$
avec dét $M(k) = k! \times (k-1)! \times (k-2)! \times ..... \times 1! \neq 0$
donc on peut inverser $M(k)$
et on obtient : $C(k) = M(k)^{-1} \times Q(k)$
en multipliant par $k!$ on obtient :
k $!\times C(k) = k! \times M(k)^{-1} \times Q(k)$
De plus, on sait que : pgcd $(c_0, c_1, ..., c_k)$ =pgcd$(C(k)) = 1$
donc pgcd $(k! \times C(k)) = k!$
donc pgcd $(k! \times M(k)^{-1} \times Q(k)) = k!$
or $k! \times M(k)^{-1} = \frac{k!}{k! \times (k-1)! ..... \times 1!} \times (\text{com}M(k))^t$

soit $k! \times M(k)^{-1} = \frac{1}{(k-1)! \times ..... \times 1!} \times$
$$\begin{pmatrix} . & . & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & . \\ . & . & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & . \\ . & . & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & . \\ . & . & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & . \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ . & . & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & . \\ . & . & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & . \\ . & . & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & . \\ . & . & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \pm(k-1)! \times ..... \times 1 \end{pmatrix}$$

donc $k! \times M(k)^{-1}$ n'est pas multiple de $k, k-1, ..., 2$
donc pgcd $(Q(k)) = k!$
donc $d(\mathbb{Z}, P)$ divise $k!$.

•

2.3 Produit des différences deux à deux.

Théorème 4 *Soient* $a_0, a_1, ..., a_n \in \mathbb{Z}$
alors

$$\prod_{0 \leq i < j \leq n} (a_i - a_j)$$

est un multiple de $1! \times ..... \times n!$.

Remarque 2 *La constante* $1! \times ..... \times n!$ *ne peut être améliorée.*

Preuve de la remarque 2 :
Si $a_0 = 0$,
$a_1 = 1$,
$a_2 = 2$,
.
.
.
$a_n = n$
on trouve facilement que :

$$\begin{aligned}\prod_{0\leq i<j\leq n}(a_j - a_i) &= [n \times (n-1) \times ..... \times 1] \times [(n-1) \times (n-2) \times ..... \times 1] \times ..... \times [2 \times 1] \times [1] \\ &= n! \times (n-1)! \times ..... \times 2! \times 1!\end{aligned}$$

•

$*$ S'il existe $a_i = a_j$ alors $\prod_{0\leq i<j\leq n}(a_j - a_i) = 0$ et est donc multiple de $1! \times ..... \times n!$.
$*$ Sinon, on peut supposer $a_0 = 0$
puisque si $a_i = \alpha_i - a_0$ alors $a_i - a_j = \alpha_i - \alpha_j$ avec $a_0 = 0$
d'où

$$\prod_{0\leq i<j\leq n}(a_i - a_j) = \prod_{1\leq j\leq n}(a_j) \times \prod_{1\leq i<j\leq n}(a_i - a_j) \quad \text{où} \quad a_i < a_j \quad \text{et} \quad a_1 \neq 0.$$

Supposons $\prod_{1\leq i<j\leq n}(a_i - a_j)$ est un multiple de $1! \times ..... \times (n-1)!$.
Il nous reste à montrer la divisibilité par $n!$.

Véracité du théorème 4 dans le cas n=2 :
Pour $n = 2$, on a :

$$\begin{aligned}\prod_{0\leq i<j\leq 2}(a_i - a_j) &= \prod_{1\leq j\leq 2}(a_j) \times \prod_{1\leq i<j\leq 2}(a_i - a_j) \\ &= a_1 \times a_2 \times (a_1 - a_2)\end{aligned}$$

Montrons que $a_1 \times a_2 \times (a_1 - a_2)$ est multiple de $2!$.
Deux cas se présentent :
$*$ soit il y a au moins un pair parmi a_1, a_2,
$*$ soit la différence $(a_1 - a_2)$ est pair.
dans les deux cas, $a_1 \times a_2 \times (a_1 - a_2)$ est pair
donc $a_1 \times a_2 \times (a_1 - a_2)$ est multiple de $2!$.
donc $\prod_{0\leq i<j\leq 2}(a_i - a_j)$ est multiple de $1! \times 2!$

•

Véracité du théorème 4 dans le cas n=3 :
Pour $n = 3$, on a :

$$\begin{aligned}\prod_{0\leq i<j\leq 3}(a_i - a_j) &= \prod_{1\leq j\leq 3}(a_j) \times \prod_{1\leq i<j\leq 3}(a_i - a_j) \\ &= a_1 \times a_2 \times a_3 \times (a_1 - a_2) \times (a_1 - a_3) \times (a_2 - a_3)\end{aligned}$$

Montrons que $a_1 \times a_2 \times a_3 \times (a_1 - a_2) \times (a_1 - a_3) \times (a_2 - a_3)$ est multiple de 3!.
Deux cas se présentent :
$*$ il n' y a aucune équivalence mod 3 parmi a_1, a_2, a_3
alors l'un d'entre eux est multiple de 3,
$*$ il y a une équivalence mod 3 parmi a_1, a_2, a_3
alors il existe une différence qui est multiple de 3.
et dans les deux cas :
$-$ soit un nombre pair figure parmi a_1, a_2, a_3
alors

$$\begin{aligned}\prod_{1\leq j\leq 3}(a_j) \times \prod_{1\leq i<j\leq 3}(a_i - a_j) &= K \times 2 \times 3 \times (1! \times 2!) \\ &= K \times 1! \times 2! \times 3!\end{aligned}$$

$-$ soit il y a 3 nombres impairs
alors

$$\begin{aligned}\prod_{1\leq j\leq 3}(a_j) \times \prod_{1\leq i<j\leq 3}(a_i - a_j) &= K \times 3 \times 2^2 \times (1! \times 2!) \\ &= K' \times 1! \times 2! \times 3!\end{aligned}$$

donc $\prod_{0\leq i<j\leq 3}(a_i - a_j)$ est multiple de $1! \times 2! \times 3!$.

•

La généralisation à n quelconque sera aisée grâce aux fonctions factorielles généralisées.

2.4 Nombre de fonctions polynômiales.

Autre exemple de fonctions factorielles en combinatoire.
Rappelons nous que, pour tout n premier, toute fonction de $\mathbb{Z}/n\mathbb{Z}$ vers $\mathbb{Z}/n\mathbb{Z}$ peut être représentée par un polynôme.Ceci parce que, quand n est premier, $\mathbb{Z}/n\mathbb{Z}$ est un corps ce qui implique que tout élément non nul a un inverse, ce qui est indispensable dans l'interpolation polynômiale de Lagrange qui nécéssite de diviser.Mais, si n n'est pas premier, $\mathbb{Z}/n\mathbb{Z}$ n' est pas un corps et toute fonction de $\mathbb{Z}/n\mathbb{Z}$ vers $\mathbb{Z}/n\mathbb{Z}$ n'a pas forcément une représentation polynômiale.

Théorème 5 (INTERPOLATION POLYNOMIALE DE LAGRANGE)
Soient des réels distincts : $x_0 < x_1 < ..... < x_n$,
soient $\alpha_i \in \mathbb{R}$ *et* $0 \leq i \leq n$,
alors il existe un polynôme de degré $\leq n$ *tel que* $P(x_i) = \alpha_i$
$P = \sum_{i=0}^{n} \alpha_i L_i$ *où les* L_i *sont des polynômes satisfaisant :*

$$L_i(x_j) = \begin{cases} 1 & si\ i = j \\ 0 & si\ i \neq j \end{cases}$$

et

$$L_i(x) = \prod_{j=0, j\neq i}^{n} \frac{x - x_j}{x_i - x_j}$$

Pour $f \in C^{n+1}([a,b])$ *on note* L_f *le polynôme de degré* $\leq n$ *tel que*

$$P(x_i) = L_f(x_i) = f(x_i) = \alpha_i \quad où\ 0 \leq i \leq n$$

Combien de fonctions de $\mathbb{Z}/n\mathbb{Z}$ vers $\mathbb{Z}/n\mathbb{Z}$ sont représentables par un polynôme ?
La formule qui donne le nombre de telles applications polynômiales fut découverte par KEMPNER en 1920 :

Théorème 6 *Le nombre de fonctions polynômiales de* $\mathbb{Z}/n\mathbb{Z}$ *vers* $\mathbb{Z}/n\mathbb{Z}$ *(équivalent au nombre de fonctions polynômiales de* $\mathbb{Z}$ *vers* $\mathbb{Z}/n\mathbb{Z}$*) est donné par :*

$$\prod_{k=0}^{n-1} \frac{n}{pgcd(n, k!)}$$

En particulier, quand n est premier, ce théorème 6 nous dit qu'il y a n^n fonctions polynômiales d'où, dans ce cas, toute fonction de $\mathbb{Z}/n\mathbb{Z}$ vers $\mathbb{Z}/n\mathbb{Z}$ est polynômiale comme on pouvait s'y attendre.

Véracité du théorème 6 dans les cas n=2 et n=3 :
On vient de voir que quand n est premier le nombre de fonctions polynômiales de $\mathbb{Z}/n\mathbb{Z}$ vers $\mathbb{Z}/n\mathbb{Z}$ est n^n,
$*$Pour $n = 2 \rightarrow 4$ fonctions polynômiales :
$P(x) = 0$,
$P(x) = 1$,
$P(x) = x$,
$P(x) = 1 + x$.
$*$Pour $n = 3 \rightarrow 3^3 = 27$ fonctions polynômiales :
$P(x) = 0$,
$P(x) = 1$,
$P(x) = 2$,
.

.
.
$P(x) = 2x^2 + 2x + 2$.

•

Véracité du théorème 6 dans le cas n=4 :
Dans ce cas, on peut remarquer les égalités des polynômes :
$* \ 2x^2 = 2x$
en effet
$x = 0 \rightarrow 2 \times 0^2 = 2 \times 0$
$x = 1 \rightarrow 2 \times 1^2 = 2 \times 1$
$x = 2 \rightarrow 2 \times 2^2 = 2 \times 4 = 8 \equiv 4 \pmod 4$ et $2 \times 2 = 4$
.
.
.
$* \ 2x^3 = 2x$
en effet

$$\begin{aligned} 2x^3 &= 2x^2 \times x \\ &= 2x \times x \\ &= 2x^2 \\ &= 2x \end{aligned}$$

et par les mêmes raisonnements on a :
$* \ 3x^2 = x^2 + 2x$
$* \ 3x^3 = x^3 + 2x$
d'où $\frac{4^4}{4} = 64$ fonctions polynômiales
ce qui correspond bien à :

$$\begin{aligned} \prod_{k=0}^{3} \frac{4}{pgcd(4, k!)} &= \frac{4}{1} \times \frac{4}{1} \times \frac{4}{2} \times \frac{4}{2} \\ &= \frac{4^4}{4} \\ &= 64 \end{aligned}$$

•

Comme pour le théorème 4, ce théorème peut être prouvé pour tout n grâce aux fonctions factorielles généralisées.

Chapitre 3

ET SI $\mathbb{Z}$ ETAIT REMPLACE PAR UN SOUS-ENSEMBLE DE $\mathbb{Z}$?

3.1 Introduction.

En résumé nous avons 4 résultats de la théorie des nombres dans lesquels la fonction factorielle joue un rôle prépondérant.Mais tous ces résultats impliquant les fonctions factorielles sont largement dépendants du fait que nous travaillons dans $\mathbb{Z}$.
En effet :
− au théorème 3 nous prenons le pgcd$(f(a) : a \in \mathbb{Z})$.
− au théorème 4 nous choisissons $(n+1)$ entiers appartenant à $\mathbb{Z}$.
− au théorème 6 nous prenons les fonctions polynômiales de $\mathbb{Z}$ vers $\mathbb{Z}/n\mathbb{Z}$.
Que se passerait-il si on changeait $\mathbb{Z}$ par un autre ensemble ?
Par exemple par un sous-ensemble S de $\mathbb{Z}$?
Ou par quelconque autre anneau ?
Ou par un sous-ensemble de quelconque autre anneau ?
Y a t'il d'autres fonctions (généralisations de la fonction factorielle) où nous pouvons changer chacun de ces $n!$ de sorte que les théorèmes 2, 3, 5 et 6 restent vrais ?
Cela nous renvoie à l'existence d' **une fonction factorielle généralisée** pour un sous-ensemble S donné de $\mathbb{Z}$ qui laisserait vrais les théorèmes 2, 3, 5 et 6.
En fait, ces théorèmes restent vrais également pour un sous-ensemble d' un anneau de DEDEKIND grâce à cette fonction factorielle généralisée.

Définition 2 *Un anneau de Dedekind est un anneau Noetherien, localement principal, dans lequel tout nombre premier différent de zéro est maximal.*

Comment construire cette fonction factorielle généralisée ?
Pour cela, nous avons besoin de la théorie du p-ordre.

3.2 Un jeu appelé p-ordre.

Soit S un sous-ensemble de $\mathbb{Z}$.
Soit p premier.
Un p-ordre de S est une suite $\{a_i\}_{i=0}^{i=\infty}$ d' éléments de S obtenue comme suit :
$*$ choisir $a_0 \in S$
$*$ choisir $a_1 \in S$ qui minimise la plus grande puissance de p divisant $(a_1 - a_0)$
$*$ choisir $a_2 \in S$ qui minimise la plus grande puissance de p divisant $(a_2 - a_0) \times (a_2 - a_1)$
.
.
.
et en général à la k^{ieme} étape :
$*$ choisir $a_k \in S$ qui minimise la plus grande puissance de p divisant $(a_k - a_0) \times (a_k - a_1) \times ..... \times (a_k - a_{k-1})$.

Notons qu'un p-ordre de S n'est certainement pas unique, en effet a_0 est choisi arbitrairement et à chaque étape suivante il y a plusieurs possibilités pour les éléments qui atteignent le minimum désiré, et nous devons choisir l'une d'entre elles à chaque étape.Au total, à chaque fois que l'on choisit un a_k cela influe sur les choix suivants.
Lorsqu'un tel p-ordre $\{a_i\}_{i=0}^{i=\infty}$ a été construit, on obtient une suite correspondante croissante $\{v_k(S,p)\}_{k=0}^{k=\infty}$ de puissances de p, où le k^{ieme} élément $\{v_k(S,p)\}$ est la puissance de p ayant minimisé à la k^{ieme} étape le processus du p-ordre.
Plus précisément, notons $w_p(a)$ la plus grande puissance de p divisant a.

Exemple 1 $w_3(18) = 9$
en effet

$$\begin{aligned} 18 &= 2 \times 3 \times 3 \\ &= 2 \times 3^2 \end{aligned}$$

donc

$$\begin{aligned} w_3(18) &= 3^2 \\ &= 9 \end{aligned}$$

•

On obtient alors

$$v_k(S,p) = w_p[(a_k - a_0) \times (a_k - a_1) \times ..... \times (a_k - a_{k-1})]$$

Nous appellerons cette suite $\{v_k(S,p)\}$ la p-suite associée à S correspondant au choix du p-ordre $\{a_i\}_{i=0}^{i=\infty}$ de S.
Deux exemples détaillés de p-ordre sont donnés dans $\mathbb{Z}$ au paragraphe 3.3 puis après l'énoncé du théorème 10 au paragraphe 4.3.
Maintenant, il semble que, puisque il y a plusieurs choix pour construire le p-ordre et puisque chaque choix influe sur les choix futurs, la p-suite associée est dépendante de ces choix.
En réalité :

Théorème 7 *La p-suite associée de S est indépendante du choix du p-ordre.*

Donc la p-suite associée dépend seulement de S, et nous pouvons parler de p-suite sans pour autant faire référence à un p-ordre particulier.
Le théorème 7 n'est pas évident à priori cependant après avoir démontré d'autres théorèmes il le deviendra.
C'est pourquoi nous le démontrerons ultérieurement.

3.3 P-ordre dans $\mathbb{Z}$.

Proposons un exemple simple de p-ordre lorsque $S = \mathbb{Z}$.

Proposition 1 *L'ordonnancement naturel $0, 1, 2, ...$ des entiers naturels forme un p-ordre de $\mathbb{Z}$ pour tout p premier.*

Preuve de la proposition 1 :
La preuve se fait par récurrence.
Supposons que $0, 1, 2, ..., k-1$ est un p-ordre jusqu'à la $(k-1)^{ieme}$ étape,(en effet le choix de 0 n'est pas considéré comme une étape, la première étape est le choix de 1) alors à la k^{ieme} étape nous devons choisir a_k qui minimise la plus grande puissance de p divisant :

$$(a_k - 0) \times (a_k - 1) \times (a_k - 2) \times ..... \times (a_k - (k-1)) \qquad (3.1)$$

Cependant notons que (3.1) est le produit de k entiers consécutifs par conséquent il doit être multiple de $k!$(d'après le théorème 2).
Mais $k!$ peut en fait être complété par le choix de $a_k = k$, d'où (3.1) devient :

$$k \times (k-1) \times (k-2) \times ..... \times (k - (k-1))$$

Cette valeur de a_k minimise manifestement la plus grande puissance de p divisant (3.1) pour tout p premier(car $k!$ est le plus petit multiple de $k!$).
Donc à la k^{ieme} étape nous choisissons $a_k = k$ et la proposition 1 en est déduite par récurrence.

•

Maintenant puisque tout p-ordre donne la même p-suite associée (d'après le théorème 7 que nous démontrerons par la suite) nous pouvons calculer la p-suite associée $v_k(S,p)$ de $\mathbb{Z}$.
Nous avons

$$\begin{aligned} v_k(S,p) &= w_p[(a_k - a_0) \times (a_k - a_1) \times ..... \times (a_k - a_{k-1})] \\ &= w_p[(k-0) \times (k-1) \times ..... \times (k-(k-1))] \\ &= w_p[k \times (k-1) \times ..... \times 1] \\ &= w_p[k!] \end{aligned}$$

En fait, si nous prenons l'expression $w_p(k!)$ et nous la multiplions par tous les p premiers alors nous obtenons exactement $k!$.

Exemple 2 $k! = 720$
Montrons que $\prod_p w_p(720!) = 720$.
on sait que

$$\begin{aligned} 720 &= 1 \times 2 \times 3 \times 4 \times 5 \times 6 \\ &= 1 \times 2 \times 3 \times 2^2 \times 5 \times 2 \times 3 \\ &= 1 \times 2^4 \times 3^2 \times 5 \end{aligned}$$

donc

$$\begin{aligned} w_2(720) &= 2^4 \\ &= 16 \\ w_3(720) &= 3^2 \\ &= 9 \\ w_5(720) &= 5 \end{aligned}$$

donc

$$\begin{aligned} \prod_p w_p(720!) &= 16 \times 9 \times 5 \\ &= 720 \end{aligned}$$

•

D'où on obtient la définition de la fonction factorielle suivante :

Définition 3

$$k! = \prod_{p,\ p\ premier} v_k(\mathbb{Z}, p)$$

Mais plus généralement nous avons la définition suivante :

Définition 4

$$k!_S = \prod_{p,\ p\ premier} v_k(S,p)$$

$k!_S$ *est appelée* ***fonction factorielle généralisée****.*

Proposition 2

$$k!_{\mathbb{Z}} = k!$$

Preuve de la proposition 2 :
La preuve sera faite au chapitre 8 à l'aide du lemme 4 énoncé dans ce même chapitre.

•

Chapitre 4

QUELQUES THEOREMES REVISITES.

Dans ce qui suit nous allons étendre les théorèmes 2, 3, 4 et 6 à un ensemble $S \subseteq \mathbb{Z}$.

4.1 Enoncé de l'extension du théorème 2.

Etendons d'abord le théorème 2.

Théorème 8 *Soient $k, l \in \mathbb{N}$*
alors $(k+l)!_S$ est un multiple de $k!_S \times l!_S$

Ce qui implique, en particulier, que nous pouvons associer un ensemble canonique de coefficients binômiaux à chaque ensemble $S \subseteq \mathbb{Z}$ par

$$\left(\begin{array}{c} n \\ k \end{array} \right)_S = \frac{n!_S}{k!_S \times (n-k)!_S}.$$

Ces coefficients du binôme généralisés ont des propriétés très intéréssantes. Le théorème 8 n'est pas aussi évident que le résultat qu'il généralise (théorème 2), en effet, comme pour le théorème 7, en essayant de prouver ce résultat directement à partir des définitions on relève un défi en exercices de combinatoire ! Nous démontrerons ce théorème dans le prochain chapitre grâce à d'autres théorèmes.

4.2 Enoncé de l'extension du théorème 3.

Le théorème 3 concernait le pgcd $d(\mathbb{Z}, f)$ des valeurs prises par un polynôme primitf f sur $\mathbb{Z}$, plus généralement :

Définition 5 *Soit f un polynôme à coefficients entiers*
alors $d(S, f)$= pgcd (f(a) : $a \in S$)
$d(S, f)$ est appelé le diviseur fixe de f sur S.

Nous pouvons nous poser la même question qu'au paragraphe 2.2 à savoir :
$*$ Quelles sont les valeurs possibles de $d(S, f)$ pour un polynôme primitif f ?

Théorème 9 *Soit f un polynôme primitif de dégré k,*
alors $d(S, f)$ divise $k!_S$.

Remarque 3 *Comme au théorème 3, $k!_S$ peut être atteint.*

Donc le théorème 9 étend le résultat de POLYA à un ensemble plus général.

4.3 Enoncé de l'extension du théorème 4.

Supposons que nous ayons choisi nos $(n+1)$ entiers non pas dans $\mathbb{Z}$ mais dans S.
Que peut-on alors dire du produit de leurs différences deux à deux ?

Théorème 10 *Soient $a_0, a_1, ..., a_n \in S$*
alors

$$\prod_{0 \leq i < j \leq n} (a_i - a_j)$$

est un multiple de $1!_S \times ..... \times n!_S$.

Remarque 4 *Comme au théorème 4 la constante $1_S! \times ..... \times n!_S$ ne peut être améliorée.*

Prenons un exemple simple :

Exemple 3 *Supposons que S est l'ensemble des nombres premiers de $\mathbb{Z}$.*
En utilisant l'algorithme du p-ordre, il est facile de trouver les 5 premiers factoriels de S.
En effet :
$\forall$ p premier,
$*$ choisissons $a_0 = 1 \in S$.

$*$ $a_1 \in S$-$\{1\}$ doit minimiser la plus grande puissance de p divisant $(a_1 - 1)$, or

$$\begin{aligned} 2 - 1 &= 1 \\ &= p^0 \end{aligned}$$

on peut donc choisir $a_1 = 2$.

$*$ $a_2 \in S$-$\{1, 2\}$ doit minimiser la plus grande puissance de p divisant $(a_2 - 1) \times (a_2 - 2)$,

or $\forall\ x \in S\text{-}\{1,2\}$, $(x-1)\times(x-2)$ *est multiple de de* $2!$ *(d'après le théorème 2)*
et

$$(3-1)\times(3-2)=2$$

on peut donc choisir $a_2 = 3$.

Soit $p = 2$.
$*$ $a_3 \in S\text{-}\{1,2,3\}$ *doit minimiser la plus grande puissance de* p *divisant* $(a_3-1)\times(a_3-2)\times(a_3-3)$,
or $\forall\ x \in S\text{-}\{1,2,3\}$, $(x-1)\times(x-2)\times(x-3)$ *est multiple de* 2^3
en effet,
. x étant premier (donc impair), $(x-2)$ *ne sera jamais pair*
. si $(x-1)$ *est multiple de 2 alors*
$(x-3)$ *est multiple de 4* $\Rightarrow (x-1)\times(x-2)\times(x-3)$ *est multiple de* 2^3
. si $(x-1)$ *est multiple de 4 alors*
$(x-3)$ *est multiple de 2* $\Rightarrow (x-1)\times(x-2)\times(x-3)$ *est multiple de* 2^3
et

$$\begin{aligned}(5-1)(5-2)(5-3) &= 4\times 3\times 2\\ &= 2^3\times 3\end{aligned}$$

on peut donc choisir $a_3 = 5$.

$*$ $a_4 \in S\text{-}\{1,2,3,5\}$ *doit minimiser la plus grande puissance de* p *divisant* $(a_4-1)\times(a_4-2)\times(a_4-3)\times(a_4-5)$,
or $\forall\ x \in S\text{-}\{1,2,3,5\}$, $(x-1)\times(x-2)\times(x-3)\times(x-5)$ *est multiple de* 2^4
en effet,
. x étant premier (donc impair), $(x-2)$ *ne sera jamais pair*
. si $(x-1)$ *est multiple de 2 alors*
$(x-3)$ *est multiple de 4 et* $(x-5)$ *est multiple de 2* $\Rightarrow (x-1)\times(x-2)\times(x-3)\times(x-5)$ *est multiple de* 2^4
. si $(x-1)$ *est multiple de 4 alors*
$(x-3)$ *est multiple de 2 et* $(x-5)$ *est multiple de 4* $\Rightarrow (x-1)\times(x-2)\times(x-3)\times(x-5)$ *est multiple de* 2^5
et

$$\begin{aligned}(7-1)\times(7-2)\times(7-3)\times(7-5) &= 6\times 5\times 4\times 2\\ &= 2^4\times 3\times 5\end{aligned}$$

on peut donc choisir $a_4 = 7$.

Soit $p = 3$.
$*$ $a_3 \in S$-$\{1,2,3\}$ *doit minimiser la plus grande puissance de* p *divisant* $(a_3 - 1) \times (a_3 - 2) \times (a_3 - 3)$,
or $\forall\ x \in S$-$\{1,2,3\}$, $(x-1) \times (x-2) \times (x-3)$ *est multiple de* $3! = 3 \times 2$
(d'après le théorème 2)
donc $\forall\ x \in S$-$\{1,2,3\}$, $(x-1) \times (x-2) \times (x-3)$ *est multiple de* 3
et

$$\begin{aligned}(5-1) \times (5-2) \times (5-3) &= 4 \times 3 \times 2 \\ &= 3 \times 2^3\end{aligned}$$

on peut donc choisir $a_3 = 5$.

$*$ $a_4 \in S$-$\{1,2,3,5\}$ *doit minimiser la plus grande puissance de* p *divisant* $(a_4 - 1) \times (a_4 - 2) \times (a_4 - 3) \times (a_4 - 5)$,
or $\forall\ x \in S$-$\{1,2,3,5\}$, $(x-1) \times (x-2) \times (x-3)$ *est multiple de* 3
et

$$\begin{aligned}(7-1) \times (7-2) \times (7-3) \times (7-5) &= 6 \times 5 \times 4 \times 2 \\ &= 3 \times 2^4 \times 5\end{aligned}$$

on peut donc choisir $a_4 = 7$.

Si p *est supérieur ou égal à 5, les premiers éléments du* p*-ordre peuvent être choisis égaux à :*

$1\ 2\ 3\ 5\ X$ *où* $X \equiv 4 \pmod{p}$ *(d'après DIRICHLET un tel* X *existe)*

et

$(X-1) \times (X-2) \times (X-3) \times (X-5)$ *non divisble par* p.

donc

$$\begin{aligned}w_p[(X-1) \times (X-2) \times (X-3) \times (X-5)] &= p^0 \\ &= 1\end{aligned}$$

On obtient alors pour
$*$ $p = 2 \quad a_0 = 1,\ a_1 = 2,\ a_2 = 3,\ a_3 = 5,\ a_4 = 7.$
$*$ $p = 3 \quad a_0 = 1,\ a_1 = 2,\ a_2 = 3,\ a_3 = 5,\ a_4 = 7.$
$*$ $p > 3 \quad a_0 = 1,\ a_1 = 2,\ a_2 = 3,\ a_3 = 5,\ a_4 = X \equiv 4 \pmod{p}.$
Ce qui nous permet de calculer les 5 premiers factoriels de S *sachant que*

$$\begin{aligned}k!_S &= \prod_{p,\ p\ premier} v_k(S,p) \\ &= \prod_{p,\ p\ premier} w_p[(a_k - a_0) \times (a_k - a_k - 1) \times \ldots\ldots\ldots \times (a_k - a_{k-1}]\end{aligned}$$

donc
$0!_S = 1$
$1!_S = 1$
$2!_S = 2$
$3!_S = 24$ *car*

$$w_2[(5-1)\times(5-2)\times(5-3)] = 2^3$$

$$w_3[(5-1)\times(5-2)\times(5-3) = 3^1$$

et

$$w_p[(X-1)\times(X-2)\times(X-3)] = p^0 \quad \text{où } p > 3$$

$4!_S = 48$ *car*

$$w_2[(7-1)\times(7-2)\times(7-3)\times(7-5)] = 2^4$$

$$w_3[(7-1)\times(7-2)\times(7-3)\times(7-5) = 3^1$$

et

$$w_p[(X-1)\times(X-2)\times(X-3)\times(X-5)] = p^0 \quad \text{où } p > 3$$

Par conséquent, si $a_0,\ a_1, ..., a_4$ *sont ces 5 premiers nombres, alors le théorème 10 dit que le produit de leurs différences deux à deux est un multiple de* $1\times1\times2\times24\times48 = 2304$ *alors que le théorème 4 nous dit seulement que c'est un multiple de* $1\times1\times2\times6\times24 = 288$.

•

4.4 Enoncé de l'extension du théorème 6.

Finalement considérons l'analogue du résultat de KEMPNER, le théorème 6.
Comme auparavant, quand n est premier chaque fonction d'un ensemble S de $\mathbb{Z}/n\mathbb{Z}$ vers $\mathbb{Z}/n\mathbb{Z}$ peut être représentée par un polynôme, quand n n'est pas premier cela n'est pas forcément le cas.
Combien de fonctions de S vers $\mathbb{Z}/n\mathbb{Z}$ sont polynômiales ?

Théorème 11 *Le nombre de fonctions polynômiales de* S *vers* $\mathbb{Z}/n\mathbb{Z}$ *est donné par :*

$$\prod_{k=0}^{n-1} \frac{n}{pgcd(n, k!_S)}.$$

Chapitre 5

PREUVES DES THEOREMES.

La simplicité des preuves des théorèmes 7, 8, 9, 10 et 11 est dûe aux observations suivantes :
Souvent, quand on écrit un polynôme il est plus facile d'utiliser la base factorielle descendante :

$$x^{(n)} = x \times (x-1) \times ..... \times (x-(n-1)) \quad \text{où } n \geq 1$$

et

$$x^{(0)} = 1$$

plutôt que la base usuelle : $\{x^n, \quad n \geq 0\}$.
En effet, beaucoup de calculs de différences sont basés sur d'importantes propriétés de ces polynômes $x^{(n)}$.
Cela nous amène à une définition analogue pour S.

Définition 6 *Soit* $\{a_i\}_{i=0}^{i=\infty}$ *un p-ordre de S*
alors

$$x^{(n)_{S,p}} = (x-a_0) \times (x-a_1) \times ..... \times (x-a_{n-1}) \quad \textit{où } n \geq 1$$

et

$$x^{(0)_{S,p}} = 1.$$

Notons que, dans le cas, où $S = \mathbb{Z}$ avec le p-ordre $0,\ 1,\ 2, ..., n-1, ...$ ces polynômes coïncident avec la définition usuelle de la base factorielle descendante dans $\mathbb{Z}$,
en effet,
$a_0 = 0$
$a_1 = 1$
$a_2 = 2$
.

.
.
$a_{n-1} = n - 1$
$\Rightarrow$

$$x^{(n)_{\mathbb{Z},p}} = x \times (x-1) \times ..... \times (x-(n-1)) \quad \text{où } n \geq 1$$

et

$$x^{(0)_{\mathbb{Z},p}} = 1.$$

Les factorielles descendantes généralisées peuvent être utilisées pour développer un calcul de différences dans S.
Bien que nous n'ayons pas besoin ici de tous les détails de cette théorie le résultat suivant doit être mentionné.

Lemme 1 *Soit un polynôme f sur $\mathbb{N}$ écrit sous la forme :*

$$\begin{aligned} f(x) &= c_0 + \sum_{i=1}^{k} c_i \times x^{(i)_{S,p}} \\ &= c_0 + \sum_{i=1}^{k} c_i \times (x-a_0) \times (x-a_1) \times ..... \times (x-a_{i-1}) \quad (5.1) \end{aligned}$$

alors $f \equiv 0 \pmod{p^e} \quad \Leftrightarrow \quad \forall\ 0 \leq i \leq k \quad c_i \times x^{(i)_{S,p}} \equiv 0 \pmod{p^e}$.

Preuve du lemme 1 :
($\Leftarrow$)
Si

$$\forall\ 0 \leq i \leq k \quad c_i \times x^{(i)_{S,p}} \equiv 0 \pmod{p^e}$$

alors

$$c_0 + \sum_{i=1}^{k} c_i \times (x-a_0) \times (x-a_1) \times ..... \times (x-a_{i-1}) \equiv 0 \pmod{p^e}$$

alors

$$f \equiv 0 \pmod{p^e}.$$

•

($\Rightarrow$)
Supposons que $f \equiv 0 \pmod{p^e}$
Raisonnons par l'absurde.
Supposons que certains termes $c_i \times x^{(i)_{S,p}}$ ne s'annulent pas mod p^e.
Alors soit j le plus petit indice (positif ou nul) tel que $c_j \times x^{(j)_{S,p}}$ ne s'annule pas.

Posons $x = a_j$ dans (5.1)
alors

$$\begin{aligned} f(a_j) &= c_0 + \sum_{i=1}^{k} c_i \times (a_j - a_0) \times (a_j - a_1) \times ..... \times (a_j - a_{i-1}) \\ &= c_0 + \sum_{i=1}^{k} c_i \times a_j^{(i)_{S,p}} \end{aligned}$$

Nous obtenons que tous les termes de $[\sum_{i>j}^{k} c_i a_j^{(i)_{S,p}}]$ s'annulent.

Exemple : $j = 2$
$f(a_2) = c_0 + c_1(a_2 - a_0) + c_2(a_2 - a_0) \times (a_2 - a_1) + c_3(a_2 - a_o) \times (a_2 - a_1) \times (a_2 - a_2) + c_4(a_2 - a_0)(a_2 - a_1) \times (a_2 - a_2) \times (a_2 - a_3) + c_5.....$
soit $f(a_2) = c_0 + c_1 \times (a_2 - a_0) + c_2 \times (a_2 - a_0) \times (a_2 - a_1)$.

Tandis que la minimalité de j garantit que les termes $0 \leq i < j$ s'annulent mod p^e.
Il s'ensuit que $c_j \times a_j^{(j)_{S,p}}$ s'annule aussi mod p^e.
Donc on a :

$$Aa_j = c_j \times (a_j - a_0) \times (a_j - a_1) \times ..... \times (a_j - a_{i-1}) \equiv 0 \pmod{p^e}$$

Montrons que $c_j \times (x - a_0) \times (x - a_1) \times ..... \times (x - a_{i-1}) \equiv 0 \pmod{p^e}$ $\forall\, x \in S$.
On a $a_j \in S$ qui minimise la plus grande puissance de p divisant Aa_j (définition d'un p-ordre et $\{a_i\}$ est un p-ordre).
S'il existait $x_j \in S$ tel que $Ax_j = c_j \times (x_j - a_0) \times (x_j - a_1) \times ..... \times (x_j - a_{i-1}) \not\equiv 0 \pmod{p^e}$
alors Ax_j ne serait pas multiple de p^e
et on a supposé que Aa_j est multiple de p^e
ce qui implique que ce ne serait pas a_j qui minimiserait la plus grande puissance de p divisant Aa_j
il y a donc une contradiction.
Donc

$$\nexists\, x_j \in S \text{ tel que } c_i \times (x_j - a_0) \times (x_j - a_1) \times ..... \times (x_j - a_{i-1}) \not\equiv 0 \pmod{p^e}$$

donc

$$\forall\, x \in S \quad c_j \times (x - a_0) \times (x - a_1) \times ..... \times (x - a_{i-1}) \equiv 0 \pmod{p^e}$$

donc

$$\forall\, x \in S \quad c_j \times x_j^{(j)_{S,p}} \equiv 0 \pmod{p^e}$$

contradiction avec

$$c_j \times x^{(j)_{S,p}} \not\equiv 0 \pmod{p^e}$$

donc

$$\forall\ 0 \leq i \leq k \quad c_i \times x^{(i)_{S,p}} \equiv 0 \pmod{p^e}.$$

•

Nous pouvons désormais prouver les théorèmes 8 à 11, dans l'ordre suivant.

5.1 Preuve du théorème 9.

Preuve du théorème 9 : Soit p un entier premier fixé.
On choisit un p-ordre $\{a_i\} \in S$.
Ecrivons f sous la forme :

$$\begin{aligned} f(x) &= c_0 + \sum_{i=1}^{k} c_i \times x^{(i)_{S,p}} \\ &= c_0 + c_1 \times (x - a_0) + \ldots\ldots\ldots + c_k \times [(x - a_0) \times \ldots\ldots\ldots \times (x - a_{k-1})] \end{aligned}$$

Comme f est un polynôme primitif, il y a un choix de j $(0 \leq j \leq k)$ tel que cj ne soit pas multiple de p.
En effet, si c_j était multiple de p alors pgcd$(c_0, c_1, \ldots\ldots\ldots, c_k)$ serait supérieur ou égal à p et donc f ne serait pas primitif.
Maintenant, par définition, f s'annule $\forall\ x \in S$ mod $w_p[d(S, f]$
car

$$w_p[d(S, f)] = \text{la plus grande puissance de } p \text{ divisant } (\text{pgcd}(f(a) : a \in S)$$

donc

$$\forall\ x \in S \quad f(x) \ \text{ est multiple de } \ d(S, f) = p^{\alpha} \times q^{\beta} \times r^{\gamma} \times \ldots\ldots\ldots$$

donc

$$\forall\ x \in S \quad f(x) \ \text{ est multiple de } \ w_p[d(S, f)] = p^{\alpha}$$

donc

$$\forall\ x \in S \quad f(x) \ \text{ s'annule } \pmod{w_p[d(S, f)]}.$$

Par le lemme 1,

$$\forall\ x \in S \quad c_j \times x^{(j)_{S,p}} \ \text{ s'annule } \pmod{w_p[d(S, f)]}.$$

De plus, puisque c_j est premier avec p, il s'ensuit que

$$\forall\ x \in S \quad x^{(j)_{S,p}} \ \text{ s'annule } \pmod{w_p[d(S, f)]}.$$

En particulier, posons $x = a_j$
alors

$$a_j^{(j)_S,p} \equiv 0 \pmod{w_p[d(S,f)]}$$

donc

$$w_p[d(S,f)] \text{ divise } a_j^{(j)_S,p}$$

donc

$$w_p[d(S,f)] \text{ divise } w_p[a_j^{(j)_S,p}]$$

où

$$\begin{aligned} w_p[a_j^{(j)_S,p}] &= w_p[(a_j - a_0) \times (a_j - a_1) \times ..... \times (a_j - a_{j-1})] \\ &= v_j(S,p) \\ &= w_p[\prod_p v_j(S,p)] \\ &= w_p[j!_S] \end{aligned}$$

donc, en particulier,

$$w_p[d(S,f)] \text{ divise } w_p[j!_S].$$

d'où

$$w_p[d(S,f)] \text{ divise } w_p[k!_S]$$

puisque $j!_S$ divise $k!_S$ (ceci car j est un sous multiple de k).
En multipliant, pour chaque terme p premier, on obtient que $d(S,f)$ divise $k!_S$ comme souhaité,
puisque

$$\begin{aligned} \prod_p w_p[d(S,f)] &= \prod_p p^\alpha \\ &= p^\alpha \times q^\beta \times r^\gamma \times ..... \\ &= d(S,f) \end{aligned}$$

et

$$\begin{aligned} \prod_p w_p[k!_S] &= \prod_p w_p[(a_k - a_0) \times (a_k - a_1) \times ..... \times (a_k - a_{k-1})] \\ &= \prod_p v_k(S,p) \\ &= k!_S \end{aligned}$$

Maintenant, on veut montrer que $k!_S$ (et chacun de ses facteurs) peut réellement être atteint.
Pour cela, nous construisons des polynômes factoriels globalement descendants $B_{k,s}$ définis comme suit :

$$B_{k,s}(x) = (x - a_{0,k}) \times (x - a_{1,k}) \times ..... \times (x - a_{k-1,k})$$

où $\{a_i\}_{i=0}^{i=\infty}$ est une suite de $\mathbb{Z}$, qui pour chaque nombre premier p divisant $k!_S$, est terme à terme congruente mod $v_k(S,p)$ à un p-ordre de S.
Alors,

$$\begin{aligned} k!_S &= \prod_p v_k(S,p) \\ &= \prod_p w_p[(a_k - a_{0,k}) \times (a_k - a_{1,k}) \times ..... \times (a_k - a_{k-1,k})] \\ &= \prod_p p^\alpha \end{aligned}$$

car a_k minimise la plus grande puissance de p divisant $(a_k - a_{0,k}) \times (a_k - a_{1,k}) \times ..... \times (a_k - a_{k-1,k})$
donc

$$\begin{aligned} k!_S &= p^\alpha \times q^\beta \times r^\gamma \times ..... \\ &= pgcd(B_{k,s}(a) : a \in S) \\ &= d(S, B_{k,s}) \end{aligned}$$

De plus, $\forall\ r$ divisant $k!_S$ on a :

$$\begin{aligned} d(S, B_{k,s} + r) &= pgcd(B_{k,s}(x) + r : x \in \mathbb{Z}) \\ &= pgcd((x - a_{0,k}) \times (x - a_{1,k}) \times ..... \times (x - a_{k-1,k}) + r : x \in \mathbb{Z}) \\ &= pgcd(r, B_{k,s}(x) : x \in \mathbb{Z}) \end{aligned}$$

or

$$\text{pgcd}(B_{k,s}(x) : x \in \mathbb{Z}) = k!_S$$

donc

$$d(S, B_{k,s} + r) = \text{pgcd}(r, k!_S)$$

et comme r divise $k!_S$
alors

$$\forall\ x \in \mathbb{Z} \quad r \ \text{ divise } \ B_{k,s}(x)$$

on obtient :

$$d(S, B_{k,s} + r) = r.$$

Donc chaque facteur de $k!_S$ peut être obtenu comme un diviseur fixe d'un certain polynôme primitif f.

•

Le théorème 9 s'avère être un outil très puissant dans la compréhension des factorielles généralisées.
Par exemple, il peut être utilisé pour donner une preuve du théorème 8.

5.2 Preuve du théorème 8.

Preuve du théorème 8 :
Par le théorème 9, il existe des polynômes primitifs f_k (ex :$B_{k,s}$) et f_{n-k} (ex :$B_{n-k,s}$) respectivement de degré k et $(n-k)$ tel que :

$$\begin{cases} d(S, f_k) = k!_S \\ d(S, f_{n-k}) = (n-k)!_S \end{cases}$$

Par multiplication, nous obtenons un polynôme primitif $f = f_k \times f_{n-k}$ de degré n tel que $k!_S \times (n-k)!_S$ divise $d(S, f_k \times f_{n-k})$
soit tel que $k!_S \times (n-k)!_S$ divise $d(S, f)$.
Mais toujours par le théorème 9, nous savons que $d(S, f)$ divise $n!_S$
donc $k!_S \times (n-k)!_S$ divise $n!_S$.
Ce qui implique, en posant $l = n - k$,
$k!_S \times l!_S$ divise $(k+l)!_S$ comme souhaité.

•

5.3 Preuve du théorème 10.

Une autre propriété importante des fonctions factorielles généralisées est donnée dans le lemme suivant :

Lemme 2 *Soit* $T \subseteq S$
alors $k!_S$ *divise* $k!_T$.

Preuve du lemme 2 :
Pour tout polynôme f on a :

$$d(S, f) \text{ divise } d(T, f) \quad (T \text{ est un sous multiple de } S)$$

d'où, en particulier,

$$d(S, B_{k,s}) = k!_S \text{ divise } d(T, B_{k,s})$$

et d'après le théorème 9 :

$$d(T, B_{k,s}) \text{ divise } k!_T$$

donc

$$k!_S \text{ divise } k!_T.$$

•

Ce lemme 2 est utilisé pour une preuve rapide du théorème 10.

Preuve du théorème 10 : Soit p premier fixé.
Supposons que $a_0, a_1, ..., a_n$ sont les $(n+1)$ premiers éléments d'un p-ordre de l'ensemble $T = \{a_0, a_1, ..., a_n\}$.
Alors puisque pour chaque $0 \leq k \leq n$

$$v_k(T,p) = w_p[(a_k - a_0) \times (a_k - a_1) \times ..... \times (a_k - a_{k-1})]$$

Nous trouvons, en prenant le produit sur tous les k puis sur tous les p :

$$1!_T \times 2!_T \times ..... \times n!_T = \pm \prod_{0 \leq i < j \leq n} (a_i - a_j)$$

car

$$\begin{aligned} \prod_{k=0}^{n} \prod_{p} v_k(T,p) &= \prod_{k=0}^{n} k!_T \\ &= 1!_T \times 2!_T \times ..... \times n!_T \end{aligned}$$

et

$$\begin{aligned} \prod_{k=0}^{n} \prod_{p} w_p[(a_k - a_0) \times (a_k - a_1) \times ... \times (a_k - a_{k-1})] &= \prod_{k=0}^{n} (a_k - a_0) \times (a_k - a_1) \times ... \times (a_k - a_{k-1}) \\ &= \pm \prod_{0 \leq i < j \leq n} (a_i - a_j) \end{aligned}$$

Maitenant, par le lemme 2, nous savons que $k!_S$ divise $k!_T$
donc

$$1!_S \times 2!_S \times ..... \times n!_S \text{ divise } 1!_T \times 2!_T \times ..... \times n!_T$$

soit

$$1!_S \times 2!_S \times ..... \times n!_S \text{ divise } \prod_{0 \leq i < j \leq n} (a_i - a_j) \text{ comme souhaité.}$$

Maintenant, montrons que la constante $1!_S \times 2!_S \times ..... \times n!_S$ ne peut être améliorée.
Remarquons que T est l'ensemble des $(n+1)$ premiers éléments d'un p-ordre de S
alors

$$\begin{aligned} w_p[\prod_{0 \leq i < j \leq n} (a_i - a_j)] &= v_0(S,p) \times v_1(S,p) \times ..... \times v_n(S,p) \\ &= \prod_{k=0}^{n} v_k(S,p) \\ &= w_p[\prod_{k=0}^{n} \prod_{p} v_k(S,p)] \\ &= w_p[\prod_{k=0}^{n} k!_S] \\ &= w_p[1!_S \times 2!_S \times ..... \times n!_S] \end{aligned}$$

donc $1!_S \times 2!_S \times ..... \times n!_S$ ne peut être remplacée par une valeur plus grande dans l'énoncé du théorème 10 .

•

5.4 Preuve du théorème 11.

Pour la preuve du théorème 11 nous avons besoin du lemme suivant :

Lemme 3 *Soit f un polynôme de degré d écrit sous la forme :*

$$\begin{aligned} f(x) &= b_0 + \sum_{k=1}^{d} b_k \times x^{(k)_{S,p}} \\ &= b_0 + \sum_{k=0}^{d} b_k \times (x-a_0) \times (x-a_1) \times ..... \times (x-a_{k-1}) \end{aligned}$$

alors $f \equiv 0 \pmod{p^e} \Leftrightarrow \forall\, 0 \leq k \leq d \;\; b_k$ *est un multiple de* $\frac{p^e}{pgcd(p^e, k!_S)}$.

Preuve du lemme 3 :
Par le lemme 1,

$$f \equiv 0 \pmod{p^e} \Leftrightarrow \forall\, 0 \leq k \leq d \;\; \forall\, x \in S \;\; b_k \times x^{(k)_{S,p}} \equiv 0 \pmod{p^e}$$

Maintenant, par construction de $x^{(k)_{S,p}}$ on a :

$$\begin{aligned} v_k(S,p) &= w_p[(a_k-a_0) \times (a_k-a_1) \times ..... \times (a_k-a_{k-1})] \\ &= p^\alpha \end{aligned}$$

et

$$\begin{aligned} w_p[d(S, x^{(k)_{S,p}})] &= w_p[d(S, (x-a_0) \times (x-a_1) \times ..... \times (x-a_{k-1}))] \\ &= w_p[pgcd((x-a_0) \times (x-a_1) \times ..... \times (x-a_{k-1})) \quad : x \in S] \\ &= p^\beta \end{aligned}$$

or

$$p^\beta \leq p^\alpha \;\; \text{car} \;\; a_k \in S$$

et

$p^\beta \not< p^\alpha$ car a_k minimise la plus grande puissance de p divisant $(a_k-a_0)\times(a_k-a_1)\times..\times(a_k-a_{k-1})$

donc

$$p^\alpha = p^\beta$$

donc on a

$$w_p[d(S, x^{(k)_{S,p}})] = v_k(S,p)$$

d'où
$\forall\ 0 \leq k \leq d \quad \forall\ x \in S \quad b_k \times x^{(k)_{S,p}} \equiv 0 \pmod{p^e} \Leftrightarrow \forall\ 0 \leq k \leq d \quad b_k$ est un multiple de $\frac{p^e}{pgcd(p^e, k!_S)}$.
en effet,

$$\begin{aligned} b_k &= \delta \frac{p^e}{pgcd(p^e, \prod_p v_k(S,p))} \\ &= \delta \frac{p^e}{pgcd(p^e, v_k(S,p))} \\ &= \delta \frac{p^e}{pgcd(p^e, p^\alpha)} \end{aligned}$$

$\odot$ si $pgcd(p^e, p^\alpha) = p^e \leq p^\alpha$
alors

$$pgcd(p^e, p^\alpha) = p^e \quad \Leftrightarrow$$

$$\begin{aligned} b_k \times x^{(k)_{S,p}} &= \frac{\delta \times p^e}{p^e} \times (x - a_0) \times (x - a_1) \times ..... \times (x - a_{k-1}) \\ &= \delta \times (x - a_0) \times (x - a_1) \times .....(x - a_{k-1}) \\ &\geq \delta \times p^\alpha \quad \text{car } p^\alpha = w_p[(a_k - a_0) \times (a_k - a_1) \times ..... \times (a_k - a_{k-1})] \\ &\geq \delta \times p^e \quad \text{car } p^\alpha \geq p^e \end{aligned}$$

donc

$$pgcd(p^e, p^\alpha) = p^e \quad \Leftrightarrow \quad b_k \times x^{(k)_{S,p}} \equiv 0 \pmod{p^e}.$$

$\odot$ si $pgcd(p^e, p^\alpha) = p^\alpha \leq p^e$
alors

$$pgcd(p^e, p^\alpha) = p^\alpha \quad \Leftrightarrow$$

$$\begin{aligned} b_k \times x^{(k)_{S,p}} &= \frac{\delta \times p^e}{p^\alpha} \times (x - a_0) \times (x - a_1) \times ..... \times (x - a_{k-1}) \\ &\geq \frac{\delta \times p^e}{p^\alpha} \times p^\alpha \quad \text{car } p^\alpha = w_p[(a_k - a_0) \times (a_k - a_1) \times ..... \times (a_k - a_{k-1})] \\ &\geq \delta \times p^e \end{aligned}$$

donc

$$pgcd(p^e, p^\alpha) = p^\alpha \quad \Leftrightarrow \quad b_k \times x^{(k)_{S,p}} \equiv 0 \pmod{p^e}.$$

donc

$$\forall\, 0 \leq k \leq d \ \ b_k \text{ est un multiple de } \frac{p^e}{pgcd(p^e, k!_S)} \Leftrightarrow \forall\, 0 \leq k \leq d \ \ \forall\, x \in S \ \ b_k \times x^{(k)_{S,p}} \equiv 0 \pmod{p^e}$$

or

$$\forall\ 0 \leq k \leq d \quad \forall\ x \in S \quad b_k \times x^{(k)_{S,p}} \equiv 0 \pmod{p^e} \quad \Leftrightarrow \quad f \equiv 0 \pmod{p^e}$$

donc

$$\forall\ 0 \leq k \leq d \quad b_k \text{ est un multiple de } \frac{p^e}{pgcd(p^e, k!_S)} \quad \Leftrightarrow \quad f \equiv 0 \pmod{p^e}.$$

Nous pouvons désormais prouver le théorème 11.

Preuve du théorème 11 :
Par le théorème chinois, spécifier qu'une application est polynômiale sur S (mod$n$) est équivalent à spécifier l'application sur S pour chaque nombre premier divisant n. De là, on voit que la formule du théorème 11 est multiplicative, donc il suffit de vérifier ce théorème quand $n = p^e$ est puissance d'un nombre premier.
Soit $\{a_i\}$ un p-ordre de S alors nous affirmons que toute application polynômiale f de S vers $\mathbb{Z}/p^e\mathbb{Z}$ peut s'écrire uniquement sous la forme :

$$f(x) = c_0 + \sum_{k=1}^{\infty} (x - a_0) \times (x - a_1) \times ..... \times (x - a_{k-1})$$

où $0 \leq c_k < \frac{p^e}{pgcd(p^e, k!_S)}$ pour chaque $k \geq 0$.
En effet, par le lemme 3, en changeant un des coefficients de c_k par un multiple de $\frac{p^e}{pgcd(p^e, k!_S)}$ dans $f(x)$, on ne modifie pas la fonction $f(x)$, ce qui signifie que les c_k sont déterminés seulement mod$\frac{p^e}{pgcd(p^e, k!_S)}$.
On a maintenant une représentation unique pour chaque application polynômiale de S vers $\mathbb{Z}/p^e\mathbb{Z}$.
En remarquant qu'il y a $\frac{p^e}{pgcd(p^e, k!_S)}$ choix de c_k pour chaque $k \geq 0$, on obtient que le nombre d' applications polynômiales de $\mathbb{Z}/n\mathbb{Z}$ vers $\mathbb{Z}/n\mathbb{Z}$ est :

$$\prod_{k=0}^{n-1} \frac{n}{pgcd(n, k!_S)} \quad \text{où } n = p^e$$

•

5.5 Preuve du théorème 7.

Les théorèmes 8 à 11 peuvent maintenant être utilisés pour démontrer le théorème 7.

Preuve du théorème 7 :
Puisque aucun des théorèmes 9 à 11 ne mentionnent les p-ordres mais qu'ils induisent (et en fait définissent) les factorielles généralisées, la définition des factorielles donnée au chapitre 3 ne peut pas dépendre des choix d'un p-ordre.

•

De façon plus directe, une façon de voir la véracité du théorème 7 est la suivante :
pour un entier positif d et un grand entier positif p tel que $p^e > v_d(S,p)$, considérons comme un groupe additif l'ensemble G_d de tous les polynômes de $(\mathbb{Z}/p^e\mathbb{Z}\,[x])$ qui s'annule sur $S \bmod(p^e)$ et de degré inférieur ou égal à d. Alors le lemme 1 implique que, en tant que groupe abélien, G est isomorphe à $\oplus_{k=0}^{d}\ \mathbb{Z}/v_k(S,p)\mathbb{Z}$.
Ainsi les nombres $v_k(S,p)\mathbb{Z}$ (pour $0 \leq k \leq d$) forment les coefficients générant ce groupe abélien G_d.
De plus, par le théorème sur les éléments générant un groupe abélien fini, ces constantes dépendent uniquement de G_d, ce qui implique le théorème 7.

Chapitre 6

POLYNÔMES A VALEURS ENTIERES.

Quelles sont les polynômes qui, pour des antécédents entiers, ont des images entières (de $\mathbb{Z}$ dans $\mathbb{Z}$) ?
Les coefficients d'un tel polynôme ne sont pas nécéssairement entiers, puisque le polynôme $f(x) = \frac{x\times(x-1)}{2}$ qui a des coefficients non entiers (ie $\frac{1}{2}$ et $-\frac{1}{2}$) est une application de $\mathbb{Z}$ dans $\mathbb{Z}$.
En effet, le produit de 2 entiers consécutifs est divisible par 2 (d'après le théorème 2).
De même, tous les polynômes binômiaux $\left(\begin{array}{c} x \\ k \end{array}\right) = \frac{x\times(x-1)\times.....\times(x-k+1)}{k!}$ sont des applications de $\mathbb{Z}$ dans $\mathbb{Z}$.
Quelques remarques sur les polynômes binômiaux :

Remarque 5 *$k \in \mathbb{N}$ et $x \in \mathbb{Z}$.*
1/Si $0 \leq x < k$

$$\left(\begin{array}{c} x \\ k \end{array}\right) = 0 \quad \textit{car l'une des parenthèses est nulle.}$$

2/Si $x \geq k$

$$\begin{aligned} \left(\begin{array}{c} x \\ k \end{array}\right) &= \frac{x \times (x-1) \times ..... \times (x-k+1)}{k!} \\ &= \frac{x!}{k! \times (x-k)!} \in \mathbb{Z} \quad \textit{d'après le théorème 2.} \end{aligned}$$

3/Si $x < 0 \qquad x = -p \leq -1$

$$\begin{aligned} \left(\begin{array}{c} x \\ k \end{array}\right) &= \frac{-p \times (-p-1) \times ..... \times [-(p+k-1)]}{k!} \\ &= \pm\frac{(p+k-1)!}{(p-1)! \times k!} \end{aligned}$$

$$= \pm \begin{pmatrix} p+k-1 \\ k \end{pmatrix} \in \mathbb{Z}$$

Puisque pour $x < 0$

$$\begin{pmatrix} x \\ k \end{pmatrix} = \begin{pmatrix} k-1-x \\ k \end{pmatrix} \quad \textit{avec } k-1-x \geq k \geq 0$$

on pourrait ne considérer que les polynômes $\begin{pmatrix} x \\ k \end{pmatrix}$ *pour* $x \in \mathbb{N}$.

Notons que :
4/

$$\begin{pmatrix} x \\ x \end{pmatrix} = \frac{x!}{x! \times 0!} = 1$$

et
5/

$$\begin{pmatrix} x \\ 0 \end{pmatrix} = \frac{x!}{0! \times x!} = 1$$

donc $\forall\ x \in \mathbb{Z}$ *et* $\forall\ k \in \mathbb{N}$ $\begin{pmatrix} x \\ k \end{pmatrix} \in \mathbb{Z}$

Quelle est la classe des polynômes appliquant $\mathbb{Z}$ dans $\mathbb{Z}$?
En 1915, POLYA donne une réponse élégante à cette question en démontrant le résultat suivant :

Théorème 12 *Un polynôme* $P(x)$ *prend, pour des antécédents entiers, ses valeurs sur* $\mathbb{Z}$ *ssi il peut être s'écrire comme une combinaison* $\mathbb{Z}$*-linéaire de polynômes binômiaux :* $\begin{pmatrix} x \\ k \end{pmatrix}$ *où* $k \in \mathbb{N}$.

Preuve du théorème 12 :
($\Leftarrow$) Toute combinaison $\mathbb{Z}$-linéaire de polynômes binômiaux est une application de $\mathbb{Z}$ dans $\mathbb{Z}$ puisque pour un polynôme binômial : $\forall\ x \in \mathbb{Z}$ $\begin{pmatrix} x \\ k \end{pmatrix} \in \mathbb{Z}$.
($\Rightarrow$)Réciproquement :
Soit $P \in Q[x]$ un polynôme de degré n tel que $\forall\ x \in \mathbb{Z}$ $P(x) \in \mathbb{Z}$.
Montrons qu'on peut définir $(n+1)$ valeurs $(b_0, b_1, ..., b_n)$ dans $\mathbb{Z}$ telles que $P(x) = \sum_{k=0}^{n} b_k \begin{pmatrix} x \\ k \end{pmatrix}$.
Définissons $b_0 \in \mathbb{Z}$ par $b_0 = P(0)$

puis successivement pour chaque valeur j de 1 à n :
supposons que $\exists(b_0, b_1, ..., b_{j-1}) \in \mathbb{Z}\ \ \forall\ x \in\ \ \mathbb{I}0; j-1\mathbb{I}$ tels que

$$P(x) = b_0 + b_1 \left(\begin{array}{c} x \\ 1 \end{array} \right) + ... + b_{j-1} \left(\begin{array}{c} x \\ j-1 \end{array} \right) = \sum_{k=0}^{j-1} b_k \left(\begin{array}{c} x \\ k \end{array} \right).$$

Définissons b_j par $b_j = P(j) - \sum_{k=0}^{j-1} b_k \left(\begin{array}{c} j \\ k \end{array} \right)$.

$P(j) \in \mathbb{Z}$ et $\sum_{k=0}^{j-1} b_k \left(\begin{array}{c} j \\ k \end{array} \right) \in \mathbb{Z}$ donc $b_j \in \mathbb{Z}$

et $\forall\ x \in\ \mathbb{I}0; j\mathbb{I} : P(x) = \sum_{k=0}^{j} b_k \left(\begin{array}{c} x \\ k \end{array} \right)$

en effet :

pour $x < j \quad \left(\begin{array}{c} x \\ j \end{array} \right) = 0$ donc $P(x) = \sum_{k=0}^{j} b_k \left(\begin{array}{c} x \\ k \end{array} \right)$

et pour $x = j \quad P(j) = \sum_{k=0}^{j-1} b_k \left(\begin{array}{c} j \\ k \end{array} \right) + b_j \left(\begin{array}{c} j \\ j \end{array} \right)$ avec $\left(\begin{array}{c} j \\ j \end{array} \right) = 1.$

P, de degré n, peut donc s'écrire pour $(n+1)$ valeurs $0, 1, 2, ..., n$

$$P(x) = \sum_{k=0}^{n} b_k \left(\begin{array}{c} x \\ k \end{array} \right)$$

Donc

$$\forall\ x \in Z \quad P(x) = \sum_{k=0}^{n} b_k \left(\begin{array}{c} x \\ k \end{array} \right) \quad \text{avec } b_k \in Z.$$

•

Exemple 4 *Soit P un polynôme de degré 2 tel que $P(x) \in$ Z.*
$b_0 = P(0)$
$b_1 = P(1) - b_0 = P(1) - P(0)$
$b_2 = P(2) - b_0 - 2b_1 = P(2) - P(0) - 2P(1)$
soit

$$P(x) = [P(2) - P(0) - 2P(1)]\frac{x(x-1)}{2} + [P(1) - P(0)]x + P(0).$$

A la suite de la démonstration du théorème 12, POLYA s'est demandé si ce résultat pouvait être étendu à d'autres ensembles.
En 1919, POLYA répondit à cette question par l'affirmative quand S= R est l'anneau des entiers dans un corps quadratique de nombres.
OSTROWSKI, dans la même année 1919, généralisa le résultat de POLYA au cas où S= R est l'anneau des entiers dans un corps quelconque de nombres.
Dans les années suivant 1919, CAHEN, CHABERT et GILMER ont prouvés des résultats analogues pour d'autres possibilités de R cependant une

réponse pour R en général n'a jamais été obtenue.
Avec les factorielles généralisées, cependant, la réponse à la question de POLYA est assez simple à conjecturer.

A savoir, nous prenons les factoriels du dénominateur de $\begin{pmatrix} x \\ k \end{pmatrix}$ dans le théorème 12 et nous les remplaçons par les factoriels généralisés, pour le numérateur nous le remplaçons par les $b_{k,s}$ du chapitre 5.
Nous obtenons de cette façon le résultat suivant :

Théorème 13 *Un polynôme $P(x)$ prend, pour des antécédents entiers, ses valeurs sur $\mathbb{Z}$ ssi il peut être s'écrire comme une combinaison $\mathbb{Z}$-linéaire du polynôme :*

$$\frac{b_{k,s}}{k!_S} = \frac{(x - a_{0,k}) \times (x - a_{1,k}) \times ..... \times (x - a_{k-1,k})}{k!_S} \quad où\ k = 0, 1, 2, ...$$

où les $b_{k,s}$ sont les polynômes définis au chapitre 5.

Chapitre 7

EXTENSION A PLUSIEURS VARIABLES.

Beaucoup de formalismes développés dans les chapitres précédents pour étudier des polynômes à une variable peuvent être étendus au cas de plusieurs variables.
Il s'agit de donner la définition correcte de factorielles pour des sous-ensembles S de $\mathbb{Z}^n$ quand $n \geq 1$.
Une clé pour la réussite est suggérée par le théorème 10, lequel déclare que choisir a_i pour minimiser le produit

$$w_p[(a_k - a_0) \times (a_k - a_1) \times ..... \times (a_k - a_{k-1})] = v_k(S, p)$$

est équivalent à minimiser la plus grande puissance de p divisant le déterminant de VANDERMONDE :

$$\begin{vmatrix} 1 & a_0 & {a_0}^2 & \cdots & \cdots & \cdots\cdots & \cdots & \cdots & {a_0}^k \\ 1 & a_1 & {a_1}^2 & \cdots & \cdots & \cdots\cdots & \cdots & \cdots & {a_1}^k \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & a_k & {a_k}^2 & \cdots & \cdots & \cdots\cdots & \cdots & \cdots & {a_k}^k \end{vmatrix} = \prod_{0 \leq i < j \leq k} (a_i - a_j).$$

En fait, il est montré que $v_0(S, p), v_1(S, p), ..., v_k(S, p)$ donne les p-parties des diviseurs élémentaires de la matrice de VANDERMONDE.
Ceci explique la définition suivante :

Définition 7 *Soit S un sous ensemble de $\mathbb{Z}^n$*
alors pour un certain ordre $M_0, M_1, ...$ des monômes $\mathbb{Z}[x_1, ..., x_n]$, un p-ordre de S est une suite $a_0, a_1, ...$ d' éléments de S choisit successive-

ment pour minimiser la plus grande puissance de p divisant le déterminant :

$$V(a_0, a_1, ..., a_k) = \begin{vmatrix} M_0(a_0) & M_1(a_0) & \cdots & \cdots & \cdots\cdots & \cdots & \cdots & M_k(a_0) \\ M_0(a_0) & M_1(a_1) & \cdots & \cdots & \cdots\cdots & \cdots & \cdots & M_k(a_1) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ M_0(a_k) & M_1(a_k) & \cdots & \cdots & \cdots\cdots & \cdots & \cdots & M_k(a_k) \end{vmatrix}$$

La p-suite associée de S est donnée par :

$$v_k(S,p) = w_p[\frac{V(a_0, a_1, ..., a_k)}{V(a_0, a_1, ..., a_{k-1})}].$$

et le factoriel généralisé est donné par :

$$k!_S = \prod_{p,\ p\ premier} v_k(S,p).$$

On peut vérifier que la définition 7, pour $n = 1$ et l'ordre du monôme usuel $1, x, x^2, ...$, coïncide avec les notions de p-ordre, p-suite associée et factorielle généralisée données au chapitre 3.

Preuve :
Soit S un sous ensemble de $\mathbb{Z}$.
Alors pour un certain ordre $1, x, x^2, ...$ du monôme $\mathbb{Z}[x_1]$, un p-ordre de S est une suite $a_0, a_1, ...$ d' éléments de S choisit successivement pour minimiser la plus grande puissance de p divisant le déterminant :

$$V(a_0, a_1, ..., a_k) = \begin{vmatrix} 1 & x & x^2 & \cdots & \cdots & \cdots\cdots & \cdots & \cdots & x^k \\ 1 & x & x^2 & \cdots & \cdots & \cdots\cdots & \cdots & \cdots & x^k \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \end{vmatrix}$$

La p-suite associée de S est donnée par :

$$\begin{aligned} v_k(S,p) &= w_p[\frac{\prod_{0\le i<j\le k}(x_i - x_j)}{\prod_{0\le i<j\le k-1}(x_i - x_j)}] \\ &= w_p[(a_k - a_0) \times (a_k - a_1) \times ..... \times (a_k - a_{k-1})]. \end{aligned}$$

et le factoriel généralisé est donné par :

$$\begin{aligned} k!_S &= \prod_{p,\ p\ premier} w_p[(a_k - a_0) \times (a_k - a_1) \times ..... \times (a_k - a_{k-1})] \\ &= \prod_{p,\ p\ premier} v_k(S,p). \end{aligned}$$

•

De plus, tous les analogues des théorémes 7, 9 à 11 et 13 peuvent être prouvés en utilisant essentiellement les mêmes techniques.

Deuxième partie

APPLICATIONS.

Chapitre 8

QUELQUES EXEMPLES ARITHMETIQUES DE FACTORIELLES GENERALISEES.

Dans ce chapitre nous allons voir quelques exemples de fonctions factorielles généralisées.
Nous avons déjà vu cet exemple ci :

Exemple 5 *Soit* $S = \mathbb{Z}$
alors $k!_{\mathbb{Z}} = k!$

Dans l'exemple 5, il y a une suite de S qui est un p-ordre pour tout p premier (ie $0, 1, 2, ...$).
Bien qu'un tel événement soit rare pour un ensemble S quelconque, il y a plusieurs ensembles importants pour lesquels cela se produit.
De plus, dans ce cas, les factorielles deviennent particulièrement faciles à calculer.
Nous établissons ceci plus précisément dans le lemme suivant :

Lemme 4 *Soit* $\{a_i\}$ *un p-ordre de* S *pour tout p premier*
alors

$$k!_S = |(a_k - a_0) \times (a_k - a_1) \times ..... \times (a_k - a_{k-1})|.$$

Preuve du lemme 4 :
Soit $\{a_i\}$ un p-ordre de S pour tout p premier
alors

$$k!_S = \prod_p v_k(S, p)$$

$$
\begin{aligned}
&= \prod_p w_p[(a_k - a_0) \times (a_k - a_1) \times ..... \times (a_k - a_{k-1})] \\
&= |(a_k - a_0) \times (a_k - a_1) \times ..... \times (a_k - a_{k-1})|
\end{aligned}
$$

•

On peut maintenant prouver l'exemple 5 à l'aide de ce lemme 4 :

Preuve de l'exemple 5 :
Soit $\{a_i\} = 0, 1, 2, ..., k$
alors

$$
\begin{aligned}
k!_S &= (k-0) \times (k-1) \times (k-2) \times ..... \times (k-(k-1)) \\
&= k!
\end{aligned}
$$

•

8.1 Ensemble des entiers pairs.

Exemple 6 *Soit $2\mathbb{Z}$ l'ensemble des entiers pairs*
alors par le même argument que dans la proposition 1, nous trouvons que l'ordonnancement naturel $0, 2, 4, 6, ...$est un p-ordre de $2\mathbb{Z}$ pour tout p premier.
D'où par le lemme 4 :

$$k!_{2\mathbb{Z}} = 2^k \times k!$$

D'une manière similaire on obtient que l'ensemble $a\mathbb{Z} + b$ de tous les entiers égaux à b modulo a ont des factoriels donnés par :

$$k!_{a\mathbb{Z}+b} = a^k \times k!$$

Preuve de l'exemple 6 :
1/Vérifions que $0, 2, 4, 6, ..., 2k, ...$ est un p-ordre de $2\mathbb{Z}$ pour tout p premier.

La preuve se fait par récurrence.
Supposons que $0, 2, 4, 6, ..., 2k-2, ...$ est un p-ordre jusqu'à la $(k-1)^{ieme}$ étape,(en effet le choix de 0 n'est pas considéré comme une étape, la première étape est le choix de 2) alors à la k^{ieme} étape nous devons choisir a_k qui minimise la plus grande puissance de p divisant :

$$(a_k - 0) \times (a_k - 2) \times (a_k - 4) \times ..... \times (a_k - (2k-2)) \qquad (8.1)$$

Cependant notons que (8.1) est le produit de k entiers consécutivement pairs par conséquent il doit être multiple de $2^k \times k!$.

Mais $2^k \times k!$ peut en fait être complété par le choix de $a_k = 2k$, d'où (8.1) devient :

$$\begin{aligned}(2k-0)\times(2k-2)\times(2k-4)\times\ldots\ldots\ldots\times(2k-(2k-2)) &= 2k\times(2k-2)\times(2k-4)\times\ldots..\times 2\\ &= 2^k\times k\times(k-1)\times(k-2)\times....\times 1\\ &= 2^k\times k!\end{aligned}$$

Cette valeur de a_k minimise manifestement la plus grande puissance de p divisant (8.1) pour tout p premier(car $2^k \times k!$ est le plus petit multiple de $2^k \times k!$).
Donc à la k^{ieme} étape nous choisissons $a_k = 2k$
et on en déduit que $0, 2, 4, 6, \ldots\ldots\ldots, 2k, \ldots\ldots\ldots$ est un p-ordre de $2\mathbb{Z}$ pour tout p premier.

2/Prouvons que $k!_{2\mathbb{Z}} = 2^k \times k!$.

$$\begin{aligned}k!_{2\mathbb{Z}} &= (2k-0)\times(2k-2)\times(2k-4)\times\ldots\ldots\ldots\times(2k-(2k-2)) \qquad \text{par le lemme 4}\\ &= 2k\times(2k-2)\times(2k-4)\times\ldots\ldots\ldots\times 2\\ &= 2^k\times k\times(k-1)\times(k-2)\times\ldots\ldots\ldots\times 1\\ &= 2^k\times k!\end{aligned}$$

3/Vérifions que $b, a+b, 2a+b, \ldots\ldots\ldots ka+b, \ldots\ldots\ldots$ est un p-ordre de $a\mathbb{Z}+b$ pour tout p premier.

La preuve se fait par récurrence.
Supposons que $b, a+b, 2a+b, \ldots\ldots\ldots, (k-1)a+b$ est un p-ordre jusqu'à la $(k-1)^{ieme}$ étape,(en effet le choix de b n'est pas considéré comme une étape, la première étape est le choix de $a+b$) alors à la k^{ieme} étape nous devons choisir a_k qui minimise la plus grande puissance de p divisant :

$$(a_k-b)\times(a_k-(a+b))\times(a_k-(2a+b))\times\ldots\ldots\ldots\times(a_k-((k-1)a+b)) \quad (8.2)$$

Cependant notons que (8.2) est le produit de k entiers consécutivement égaux modulo a par conséquent il doit être multiple de $a^k \times k!$.
Mais $a^k \times k!$ peut en fait être complété par le choix de $a_k = ak + b$, d'où (8.2) devient :
$(a_k - b) \times (a_k - (a + b)) \times (a_k - (2a + b)) \times \ldots\ldots\ldots \times (a_k - ((k - 1) + b))$
$= (ak + b - b) \times (ak + b - (a + b)) \times ((ak + b) - (2a + b)) \times \ldots\ldots\ldots \times (ak + b - ((k - 1)a + b))$
$= (ak) \times (ak - a) \times (ak - 2a) \times \ldots\ldots\ldots \times a$
$= a^k \times k \times (k - 1) \times (k - 2) \times \ldots\ldots\ldots \times 1$
$= a^k \times k!$
Cette valeur de a_k minimise manifestement la plus grande puissance de p divisant (8.2) pour tout p premier.(car $a^k \times k!$ est le plus petit multiple de

$a^k \times k!$).
Donc à la k^{ieme} étape nous choisissons $a_k = ak + b$
et on en déduit que $b, a+b, 2a+b, ...ka+b, ...$ est un p-ordre de $a\mathbb{Z}+b$ pour tout p premier.

4/Prouvons que $k!_{a\mathbb{Z}+b} = a^k \times k!$.

$k!_{a\mathbb{Z}+b}$
$= (ak+b-b) \times (ak+b-(a+b)) \times (ak+b-(2a+b)) \times ..... \times (ak+b-((k-1)a+b))$ par le lemme 4
$= (ak) \times (ak-a) \times (ak-2a) \times ..... \times a$
$= a^k \times k \times (k-1) \times (k-2) \times ..... \times 1$
$= a^k \times k!$

•

8.2 Ensemble des puissances de 2.

Exemple 7 *Soit S l'ensemble des puissances de 2 dans $\mathbb{Z}$*
alors il est facile de vérifier que $1, 2, 4, 8, ..., 2^k, ...$ est un p-ordre de S pour tout p premier.
D'où par le lemme 4 :

$$k!_S = (2^k - 1) \times (2^k - 2) \times (2^k - 4) \times ..... \times (2^k - 2^{k-1})$$

Plus généralement, si on prend une suite géométrique de S dans $\mathbb{Z}$ de raison q et de premier terme a alors

$$k!_S = a^k \times (q^k - 1) \times (q^k - q) \times (q^k - q^2) \times ..... \times (q^k - q^{k-1})$$

Preuve de l'exemple 7 :
1/Vérifions que $1, 2, 4, 8, ..., 2^k, ...$ est un p-ordre de S pour tout p premier.

Choisissons $a_0 = 1$
Pour tout p premier, 2 minimise la plus grande puissance de p divisant $(x-1)$
car $(2-1) = 1$
donc $a_1 = 2$
Pour tout p premier, 2^2 minimise la plus grande puissance de p divisant $(x-1) \times (x-2)$
car $(4-1) \times (4-2) = 3 \times 2$
et si $x \in \left\{2^k \ ; \ k \geq 2\right\}$ $(x-1) \times (x-2)$ est multiple de 2 et 3 puisque x pair est non multiple de 3
on peut donc choisir $a_2 = 2^2$
Raisonnons par récurrence pour le choix de a_k en général.

Le choix de $a_0 = 1$ rend vraie au rang 0 la propriété à démontrer.
Supposons $a^i = 2^i$ pour tout $i \in [|0; k-1|]$
Soit

$$\begin{aligned} A_{k+j} &= (x-1) \times (x-2) \times ..... \times (x-2^{k-1}) \text{ avec } x = 2^{k+j} \text{ et } j \geq 0 \\ &= (2^{k+j}-1) \times (2^{k+j}-2) \times ..... \times (2^{k+j}-2^{k-1}) \\ &= 2 \times 2^2 \times ..... \times 2^{k-1} \times (2^{k+j}-1) \times (2^{k+j-1}-1) \times ..... \times (2^{j+1}-1) \\ &= 2^{\frac{k\times(k-1)}{2}} \times (2^{k+j}-1) \times (2^{k+j-1}-1) \times ..... \times (2^{j+1}-1) \end{aligned}$$

donc $w_2[A_{k+j}] = 2^{\frac{k\times(k-1)}{2}}$ pour tout $j \geq 0$, en particulier pour $j = 0$.
Soit p premier autre que 2 :
A_{k+j} est le produit de $2^{\frac{k\times(k-1)}{2}}$ par k parenthèses (2^l-1) où $l \in [|j+1; j+k|]$
Si $\lfloor k : p \rfloor = \alpha$, A_{k+j} sera multiple de $(2^p-1)^\alpha$ pour tout $j \geq 0$
En effet,

$$\begin{aligned} 2^{np}-1 &= (2^p)^n - 1 \\ &= (2^p-1) \times [\ ] \end{aligned}$$

Exemples
$k = 3 \quad \Rightarrow \quad A_{3+j} = 2^3 \times (2^{3+j}-1) \times (2^{2+j}-1) \times (2^{1+j}-1)$
$\lfloor 3 : 2 \rfloor = 1$ *donc* A_{3+j} *est multiple de* $(2^2-1)^1 = 3$
$\lfloor 3 : 3 \rfloor = 1$ *donc* A_{3+j} *est multiple de* $(2^3-1)^1 = 7$
A_{3+j} *est multiple de* $A_3 = 2^3 \times 3 \times 7$
on peut donc choisir $a_3 = 2^3$

$k = 4 \quad \Rightarrow \quad A_{4+j} = 2^6 \times (2^{4+j}-1) \times (2^{3+j}-1) \times (2^{2+j}-1) \times (2^{1+j}-1)$
$\lfloor 4 : 2 \rfloor = 2$ *donc* A_{4+j} *est multiple de* $(2^2-1)^2 = 3^2$
$\lfloor 4 : 3 \rfloor = 1$ *donc* A_{4+j} *est multiple de* $(2^3-1)^1 = 7$
$\lfloor 4 : 4 \rfloor = 1$ *donc* A_{4+j} *est multiple de* $(2^4-1)^1 = 15 = 3 \times 5$
A_{4+j} *est multiple de* $A_4 = 2^6 \times 3^2 \times 5 \times 7$
on peut donc choisir $a_4 = 2^4$

On montre de même que A_{5+j} est multiple de $A_5 = 2^{10} \times 3^2 \times 5 \times 7 \times 31$
et plus généralement, dans le raisonnement par récurrence, que A_{k+j} est multiple de A_k pour $j \geq 0$.
On peut donc, pour tout entier k, choisir $j = 0$.
Soit $a_k = 2^k$ alors $1, 2, 4, 8, ..., 2^k, ...$ est un p-ordre de S pour tout p premier.

2/Prouvons que $k!_S = (2^k-1) \times (2^k-2) \times (2^k-4) \times ..... \times (2^k-2^{k-1}))$

A l' aide du p-ordre et du lemme 4 on obtient directement :

$$k!_S = (2^k-1) \times (2^k-2) \times (2^k-4) \times ..... \times (2^k-2^{k-1})$$

3/On peut vérifier de même que $a, aq, aq^2, , ..., aq^k, ...$ est un p-ordre de S pour tout p premier où S est une suite géométrique de S dans $\mathbb{Z}$ de raison q et de premier terme a.

La preuve se fait par récurrence en choisissant $a_0 = 0$.
et

$$\begin{aligned} A_{k+j} &= (aq^{k+j} - aq^{k-1}) \times ..... \times (aq^{k+j} - a) \\ &= a^k \times q^{\frac{k\times(k-1)}{2}} \times (q^{k+j} - 1) \times ..... \times (q^{j+1} - 1) \\ &= a^k \times q^{\frac{k\times(k-1)}{2}} \times A'_{k+j} \end{aligned}$$

On montre, comme dans le cas $q = 2$, que pour $j \geq 0$ A'_{k+j} est multiple de A'_k
avec $A'_k = (q^k - 1) \times ..... \times (q - 1)$ puisque si $\lfloor k : p \rfloor = \alpha$
$(q^{k+j} - 1) \times ..... \times (q^{j+1} - 1)$ sera multiple de $(q^p - 1)^\alpha$
On peut, pour tout entier k, choisir $a_k = aq^k$
donc $a, aq, aq^2, , ..., aq^k, ...$ est un p-ordre de S pour tout p premier où S est une suite géométrique de S dans $\mathbb{Z}$ de raison q et de premier terme a.

4/Prouvons que $k!_S = a^k \times (q^k - 1) \times (q^k - q) \times (q^k - q^2) \times ..... \times (q^k - q^{k-1})$.

$$\begin{aligned} k!_S &= (aq^k - a) \times (aq^k - aq) \times (aq^k - aq^2) \times ..... \times (aq^k - aq^{k-1}) \qquad \text{d'après le lemme 4} \\ &= a^k \times (q^k - 1) \times (q^k - q) \times (q^k - q^2) \times ..... \times (q^k - q^{k-1}) \end{aligned}$$

•

8.3 Ensemble des carrés de $\mathbb{Z}$.

Exemple 8 *Soit S' l'ensemble des carrés de $\mathbb{Z}$*
alors on peut montrer que $0, 1, 4, 9, ..., k^2, ...$ est un p-ordre de S' pour tout p premier.
D'où par le lemme 4 :

$$k!_{S'} = \frac{(2k)!}{2}$$

Preuve de l'exemple 8 :
1/Prouvons que $0, 1, 4, 9, ..., k^2, ...$ est un p-ordre de S' pour tout p premier.

La preuve se fait par récurrence.
Choisissons $a_0 = 0$ et supposons jusqu'à la $(k-1^{ieme})$ étape le choix successif de $\{a_i\} = i^2$ avec $1 \leq i \leq k - 1$
Au rang k montrons que k^2 minimise la plus grande puissance de p divisant

$$x \times (x - 1) \times (x - 2^2) \times ..... \times (x - (k - 1)^2)$$

Soit

$$\begin{aligned} A_{k,0} &= k^2 \times (k^2-1) \times (k^2-2^2) \times ..... \times (k^2-(k-1)^2) \\ &= k \times (k-1) \times (k-2) \times ..... \times 1 \times k \times (k+1) \times (k+2) \times ..... \times (2k-1) \\ &= k[1 \times 2 \times ..... \times (k-2) \times (k-1) \times k \times (k+1) \times (k+2) \times ..... \times (2k-1)] \\ &= k \times (2k-1)! \end{aligned}$$

Montrons que $A_{k,\alpha}$ est multiple de $A_{k,0}$
où

$$\begin{aligned} A_{k,\alpha} &= (k+\alpha)^2 \times [(k+\alpha^2)-1] \times ..... \times [(k+\alpha)^2-(k-1)^2] \qquad \alpha > 0 \\ &= (k+\alpha) \times (k+\alpha-1) \times ..... \times (\alpha+1) \times (k+\alpha) \times (k+\alpha+1) \times ..... \times (2k-1+\alpha) \\ &= (k+\alpha) \underbrace{[(\alpha+1) \times ..... \times (k+\alpha-1)]}_{\equiv 0 \bmod k} (k+\alpha) \underbrace{[(k+\alpha+1) \times ..... \times (2k-1+\alpha)]}_{\equiv 0 \bmod k} \end{aligned}$$

or $(\alpha+1) \times (\alpha+2) \times ..... \times (2k-1+\alpha)$ est le produit de $2k-1$ entiers consécutifs
donc $(\alpha+1) \times (\alpha+2) \times ..... \times (2k-1+\alpha)$ est multiple de $(2k-1)!$ d'après le théorème 2
donc $A_{k,\alpha}$ est multiple de $(2k-1)!$
Et si $p+\alpha \equiv 0 \pmod{k}$ avec $k+1 \leq p+k \leq 2k-1$
alors $p+k+\alpha \equiv 0 \pmod{k}$ avec $1 \leq p \leq k-1$
donc $A_{k,\alpha}$ est multiple de k^2 pour tout $\alpha > 0$
donc $A_{k,\alpha}$ est multiple de $A_{k,0}$
donc au rang k, on peut choisir $a_k = k^2$
donc $0, 1, 4, 9, ..., k^2, ...$ est un p-ordre de S' pour tout p premier.

2/Prouvons que $k!_{S'} = \frac{(2k)!}{2}$.

$$\begin{aligned} k!_{S'} &= (k^2-0) \times (k^2-1) \times (k^2-2^2) \times ..... \times (k^2-(k-1)^2) \qquad \text{d'après le lemme 4} \\ &= [k \times k] \times [(k-1) \times (k+1)] \times [(k-2) \times (k+2)] \times ..... \times (2k-1) \\ &= k \times (k-1) \times (k-2) \times ..... \times 1 \times k \times (k+1) \times (k+2) \times ..... \times (2k-1) \\ &= k \times (k-1) \times (k-2) \times ..... \times 1 \times (k+1) \times (k+2) \times ..... \times (2k-1) \times (\frac{2k}{2}) \\ &= \frac{(2k)!}{2} \end{aligned}$$

•

8.4 Ensemble des entiers premiers de $\mathbb{Z}$.

Nous donnons ici un exemple d'un sous-ensemble S de $\mathbb{Z}$ qui ne possède pas un p-ordre identique pour tout premier p.
Par conséquent, la formule pour $k!_{S''}$ est un peu plus compliquée.

Exemple 9 *Soit S'' l'ensemble des entiers premiers de $\mathbb{Z}$*
alors pour un p premier fixé, on peut montrer que un p-ordre de S'' est donné par une suite $\{a_i\}$ ayant la propriété suivante :
pour chaque $e \geq 1$, l'ensemble $\left\{a_0, a_1, ..., a_{p^{e-1}(p-1)}\right\}$ est équivalent à $(\mathbb{Z}/p^e\mathbb{Z})^\times \cup \{p\}$ quand il est considéré $\pmod p$.
Une telle suite existe d'après le théorème de DIRICHLET.

Théorème 14 (DIRICHLET) *Soit $b \in \mathbb{Z}$ et $b \notin \{0, -1, 1\}$*
alors pour tout α $(\mathbb{Z}/b\mathbb{Z})^\times$ il existe une infinité de premiers p tels que $\bar{p} = \alpha$ dans $\mathbb{Z}/b\mathbb{Z}$ $\pmod b$

Les factoriels de S'' sont alors donnés par :

$$k!_{S''} = \prod_p p^{\left\lfloor \frac{k-1}{p-1} \right\rfloor + \left\lfloor \frac{k-1}{p(p-1)} \right\rfloor + \left\lfloor \frac{k-1}{p^2(p-1)} \right\rfloor + ...}.$$

Preuve de l'exemple 9 :
Montrons qu'un p-ordre de S'' est donné par une suite $\{a_i\}$ tel que $\forall\ e \geq 1$, l'ensemble $\left\{a_0, a_1, ..., a_{p^{e-1}(p-1)}\right\} \approx_{p^e} (\mathbb{Z}/p^e\mathbb{Z})^\times \cup \{p\}$.

1/Montrons d'abord que $\forall\ a_{p^{e-1}(p-1)} e \geq 1$ card $[(\mathbb{Z}/p^e\mathbb{Z})^\times \cup \{p\}] = p^{e-1}(p-1) + 1$.

En effet pour $n \geq 2$, $\quad x \in \mathbb{Z} \quad$ et $\quad \overline{x} \in \mathbb{Z}/n\mathbb{Z}$.
On a : $\overline{x}$ inversible dans $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow (x, n) = 1$.
Les nombres inversibles de $\mathbb{Z}/p^e\mathbb{Z}$ sont donc tous ceux qui ne sont pas multiples de p (donc premiers avec p^e)
il y en a donc $p^e - p^{e-1} = p^{e-1} \times (p-1)$
donc

$$\begin{aligned} \text{card } [(\mathbb{Z}/p^e\mathbb{Z})^\times \cup \{p\}] &= p^{e-1}(p-1) + 1 \\ &= \text{card } \left\{a_0, a_1, ..., a_{p^{e-1}(p-1)}\right\} \end{aligned}$$

2/Cherchons les éléments du p-ordre inférieurs ou égaux à p.

Si a et b sont deux éléments distincts inférieurs ou égaux à p ($\bar{a}$ et $\bar{b}$ éléments de $\mathbb{Z}/p\mathbb{Z}$)
alors $(a-b)$ n'est pas multiple de p
donc

$$\begin{aligned} w_p[a-b] &= p^0 \\ &= 1 \end{aligned}$$

Soit $\{a_0, a_1, ..., a_{p-1}\} \approx_p (\mathbb{Z}/p\mathbb{Z})$.
On peut considérer mod p les premiers termes du p-ordre comme la suite

ordonnée $(1, 2, 3, ..., p)$ avec $w_p[(p-1) \times (p-2) \times ..... \times (p-(p-1))] = p^0 = 1$.

3/Plus généralement :

Soit $a_i > p \in S''$ (a_i est un élément du p-ordre)
et $\alpha_i \in (\mathbb{Z}/p^e\mathbb{Z})^\times$
tel que $a_i \approx_{p^e} \alpha_i$
alors

$$\begin{aligned} a_i - a_j &= \alpha_i + mp^e - \alpha_j - np^e \\ &= \alpha_i - \alpha_j + (m-n)p^e \end{aligned}$$

donc
$*$ si $m = n$

$$a_i - a_j = \alpha_i - \alpha_j$$

donc

$$w_p[(a_i - a_j)] = w_p[(\alpha_i - \alpha_j)]$$

$*$ si $m \neq n$

$$a_i - a_j = \alpha_i - \alpha_j + (m-n)p^e$$

donc

$$w_p[(a_i - a_j)] = w_p[(\alpha_i - \alpha_j)] < p^e \quad \text{car} \quad \alpha_i \quad \text{et} \quad \alpha_j \quad \text{sont dans} \quad (\mathbb{Z}/p^e\mathbb{Z})^\times$$

On peut donc substituer $\alpha_i \in (\mathbb{Z}/p^e\mathbb{Z})^\times$ à tout a_i sans modifier w_p et le théorème de DIRICHLET assure l'existence de premiers équivalents à tout $\alpha_i \in (\mathbb{Z}/p^e\mathbb{Z})^\times$ pour tout p premier et tout $e \geq 1$.

4/Calculons w_p

$*$ Si $1 \leq a_k \leq p-1$
alors

$$1 \leq k \leq p-1 \quad \text{et} \quad k-1 < p-1 \quad \text{d'après 2/}$$

donc

$$\left\lfloor \frac{k-1}{p-1} \right\rfloor = 0$$

et

$$\begin{aligned} w_p[(a_k - a_0) \times (a_k - a_1) \times ..... \times (a_k - a_{k-1})] &= p^0 \\ &= 1 \end{aligned}$$

$*$ Supposons $e \geq 2$ et $p^{e-2}(p-1) \leq k-1 < p^{e-1}(p-1)$
en considérant, mod p^e, les éléments $(a_0, a_1, ..., a_{p^{e-1}(p-1)})$ d'un p-ordre

comme équivalents à $(\mathbb{Z}/p^e\mathbb{Z})^\times \cup \{p\}$ le produit $(a_k - 1) \times ..... \times (a_k - a_{k-1})$ comporte :
$\rightarrow$ un nombre de multiples de p égal à $\left\lfloor \frac{k-1}{p-1} \right\rfloor$
$\rightarrow$ un nombre de multiples de p^2 égal à $\left\lfloor \frac{k-1}{p(p-1)} \right\rfloor$
$\vdots$
en ordonnant les termes de a_k par leur représentation minimum dans $\mathbb{N}$ et

$$w_p[(a_k - a_0) \times (a_k - a_1) \times ..... \times (a_k - a_{k-1})] = p^{\left\lfloor \frac{k-1}{p-1} \right\rfloor + \left\lfloor \frac{k-1}{p(p-1)} \right\rfloor + ...}$$

exemple : $p = 3$ *et* $e = 3$
On a le p-ordre $1, 2, 3, 4, 5, 7, 8, 10, a_8$ *où* $a_8 \in \{11, 14, 17, 20, 23, 26\}$.
On a $3^1 \times 2 \leq 8 - 1 < 3^2 \times 2$
on obtient 3 multiples de 3 *dont un multiple de* 3^2
c'est à dire $w_p[(a_8 - 1) \times (a_8 - 2) \times ..... \times (a_8 - 10)] = 3^4$
ce qui vérifie bien $3^{\left\lfloor \frac{7}{2} \right\rfloor + \left\lfloor \frac{7}{6} \right\rfloor} = 3^{3+1} = 3^4$.

On peut donc considérer mod p^e, les éléments $(a_0, a_1, ..., a_{p^{e-1}(p-1)})$ d'un p-ordre comme équivalents à la suite (ordonnée croissante de $\mathbb{N}$) des éléments de $(\mathbb{Z}/p^e\mathbb{Z})^\times \cup \{p\}$ avec

$$w_p[(a_k - a_0) \times (a_k - a_1) \times ..... \times (a_k - a_{k-1})] = p^{\left\lfloor \frac{k-1}{p-1} \right\rfloor + \left\lfloor \frac{k-1}{p(p-1)} \right\rfloor + ...}$$

5/Prouvons que $k!_{S''} = \prod_p p^{\left\lfloor \frac{k-1}{p-1} \right\rfloor + \left\lfloor \frac{k-1}{p(p-1)} \right\rfloor + \left\lfloor \frac{k-1}{p^2(p-1)} \right\rfloor + ...}$.

$$\begin{aligned} k!_{S''} &= \prod_p w_p[(a_k - a_0) \times (a_k - a_1) \times ..... \times (a_k - a_{k-1})] \\ &= \prod_p p^{\left\lfloor \frac{k-1}{p-1} \right\rfloor + \left\lfloor \frac{k-1}{p(p-1)} \right\rfloor + \left\lfloor \frac{k-1}{p^2(p-1)} \right\rfloor + ...} \end{aligned}$$

•

Exemple 10 *On propose un exemple qui illustre cette formule :*
calculons $7!_{S''}$.
$*$ *Notre* 2*-ordre est :*
$a_0 = 1$
$a_1 = 2$
$a_2 = 3$
$a_3 = 5$
$a_4 = 7$
$a_5 = 9$

$a_6 = 11$
$a_7 = 13$
donc on obtient :

$$\begin{aligned}(a_7 - a_0) \times (a_7 - a_1) \times ..... \times (a_7 - a_6) &= 12 \times 11 \times 10 \times 8 \times 6 \times 4 \times 2 \\ &= 2^2 \times 3 \times 11 \times 2 \times 5 \times 2^3 \times 2 \times 3 \times 2^2 \times 2 \\ &= 2^{10} \times 3^2 \times 5 \times 11\end{aligned}$$

donc

$$w_2[(a_7 - a_0) \times (a_7 - a_1) \times ..... \times (a_7 - a_6)] = 2^{10}$$

$*$ *Notre* 3*-ordre est :*
$a_0 = 1$
$a_1 = 2$
$a_2 = 3$
$a_3 = 4$
$a_4 = 5$
$a_5 = 7$
$a_6 = 8$
$a_7 = 10$
donc on obtient :

$$\begin{aligned}(a_7 - a_0) \times (a_7 - a_1) \times ..... \times (a_7 - a_6) &= 9 \times 8 \times 7 \times 6 \times 5 \times 3 \times 2 \\ &= 3^2 \times 2^3 \times 7 \times 2 \times 3 \times 5 \times 3 \times 2 \\ &= 2^5 \times 3^4 \times 5 \times 7\end{aligned}$$

donc

$$w_3[(a_7 - a_0) \times (a_7 - a_1) \times ..... \times (a_7 - a_6)] = 3^4$$

$*$ *Notre* 5*-ordre est :*
$a_0 = 1$
$a_1 = 2$
$a_2 = 3$
$a_3 = 4$
$a_4 = 5$
$a_5 = 6$
$a_6 = 7$
$a_7 = 8$
donc on obtient :

$$\begin{aligned}(a_7 - a_0) \times (a_7 - a_1) \times ..... \times (a_7 - a_6) &= 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 \\ &= 7 \times 2 \times 3 \times 5 \times 2^2 \times 3 \times 2 \times 1 \\ &= 2^4 \times 3^2 \times 5 \times 7\end{aligned}$$

donc

$$w_5[(a_7 - a_0) \times (a_7 - a_1) \times ..... \times (a_7 - a_6)] = 5$$

$*$ *Notre* 7*-ordre est :*
$a_0 = 1$
$a_1 = 2$
$a_2 = 3$
$a_3 = 4$
$a_4 = 5$
$a_5 = 6$
$a_6 = 7$
$a_7 = 8$
donc on obtient :

$$\begin{aligned}(a_7 - a_0) \times (a_7 - a_1) \times ..... \times (a_7 - a_6) &= 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 \\ &= 7 \times 2 \times 3 \times 5 \times 2^2 \times 3 \times 2 \times 1 \\ &= 2^4 \times 3^2 \times 5 \times 7\end{aligned}$$

donc

$$w_7[(a_7 - a_0) \times (a_7 - a_1) \times ..... \times (a_7 - a_6)] = 7$$

ce qui implique

$$7!_{S''} = 2^{10} \times 3^4 \times 5 \times 7$$

Vérifions que la formule de l'exemple 9 nous donne bien le même résultat.
$p = 2 \rightarrow \left\lfloor \frac{6}{1} \right\rfloor = 6,\ \left\lfloor \frac{6}{2} \right\rfloor = 3,\ \left\lfloor \frac{6}{4} \right\rfloor = 1$
$p = 3 \rightarrow \left\lfloor \frac{6}{2} \right\rfloor = 3,\ \left\lfloor \frac{6}{6} \right\rfloor = 1$
$p = 5 \rightarrow \left\lfloor \frac{6}{4} \right\rfloor = 1$
$p = 7 \rightarrow \left\lfloor \frac{6}{6} \right\rfloor = 1$
et donc d'après la formule :

$$\begin{aligned}7!_{S''} &= 2^{6+3+1} \times 3^{3+1} \times 5^1 \times 7^1 \\ &= 2^{10} \times 3^4 \times 5 \times 7\end{aligned}$$

comme précédemment.

•

Remarque 6 *Pour M BHARGAVA* $k!_{S''} = 2^{\left\lfloor \frac{k}{2} \right\rfloor}$ *par le produit des dénominateurs des* $\left\lceil \frac{k}{2} \right\rceil$ *premiers nombres de BERNOUILLI.*
Ce résultat est inexact : les puissances associées aux nombres premiers n'étant pas toujours celles prévues par l'affirmation de M BHARGAVA.

Exemple 11 *Les premiers nombres de BERNOUILLI sont :*$1, -\frac{1}{2}, \frac{1}{6}, 0, -\frac{1}{30}, 0, \frac{1}{42}, 0.....$
donc avec le résultat de M BHARGAVA on aurait :

$$\begin{aligned}7!_{S''} &= 2^{\left\lfloor \frac{7}{2} \right\rfloor} \times 2 \times 6 \times 30 \times 42 \\ &= 2^3 \times 2 \times 2 \times 3 \times 2 \times 3 \times 5 \times 2 \times 3 \times 7 \\ &= 2^7 \times 3^3 \times 5 \times 7\end{aligned}$$

On peut donc constater le résultat suivant :

Résultat 1 *Les nombres qui apparaissent dans la décomposition de* $k!_{S''}$ *sont exactement les nombres premiers apparaissant dans les dénominateurs des* $\left\lceil \frac{k}{2} \right\rceil$ *premiers nombres de BERNOUILLI.*

Chapitre 9

LA FONCTION DE CARLITZ ET LA FONCTION FACTORIELLE GENERALISEE.

Il y a plusieurs généralisations possibles des factorielles qui peuvent être obtenues comme des cas particuliers des définitions que nous avons données.

9.1 Les Q-factorielles.

L'exemple 7 nous rappelle les q-factorielles qui apparaissent en combinatoire.
En effet on peut obtenir ces q-factorielles abstraites directement comme suit :

Exemple 12 *Soit S''' l'ensemble $\left\{\frac{q^k-1}{q-1} \ : \ k \ \in \ \mathbb{N}\right\}$ de l'anneau $\mathbb{C}[q,q^{-1}]$ alors*

$$k!_{S'''} = q^{\frac{k(k-1)}{2}} \times (q-1)^{-k} \times (q^k-1) \times (q^{k-1}-1) \times ..... \times (q-1)$$

où $(q^k-1) \times (q^{k-1}-1) \times ..... \times (q-1)$ est le k^{ieme} q-factoriel.

Remarque 7 *Il est à noter que dans la formule donnée par M BHARGAVA $q^{\frac{k(k-1)}{2}}$ n'apparaissait pas.*

Preuve de l'exemple 12 :
1/Vérifions que $0, 1, \frac{q^2-1}{q-1}, ..., \frac{q^k-1}{q-1}, ...$ est un p-ordre de S''' pour tout p premier.

La preuve se fait par récurrence.
Choisissons $a_0 = 0$ et supposons au rang $i < k$,

$$a_i = \frac{q^i - 1}{q - 1} \quad \text{pour} \quad 0 \leq i < k$$

Posons

$$\begin{aligned} B_{k+j} &= (x - \frac{q^{k-1} - 1}{q - 1}) \times (x - \frac{q^{k-2} - 1}{q - 1}) \times ..... \times x \ \text{ avec } \ x = \frac{q^{k+j} - 1}{q - 1} \ \text{ et } \ j \geq 0 \\ &= (\frac{q^{k+j} - q^{k-1}}{q - 1}) \times (\frac{q^{k+j} - q^{k-2}}{q - 1}) \times ..... \times (\frac{q^{k+j} - 1}{q - 1}) \\ &= \frac{1}{(q-1)^k} \times (q^{k+j} - q^{k-1}) \times (q^{k+j} - q^{k-2}) \times ..... \times (q^{k+j} - 1) \\ &= \frac{1}{(q-1)^k} \times q^{\frac{k \times (k-1)}{2}} \times A'_{k+j} \end{aligned}$$

où on retrouve A'_{k+j} désigné ainsi au paragraphe 8.2.
A'_{k+j} étant multiple de A'_k, on peut choisir

$$a_k = \frac{q^k - 1}{q - 1}$$

Exemple : $k = 3$

$$a_0 = 0$$

$$a_1 = \frac{q-1}{q-1} = 1$$

$$a_2 = \frac{q^2 - 1}{q - 1}$$

$$\begin{aligned} B_3 &= (\frac{q^3 - 1}{q - 1} - \frac{q^2 - 1}{q - 1}) \times (\frac{q^3 - 1}{q - 1} - \frac{q - 1}{q - 1}) \times (q^3 - 1) \\ &= \frac{1}{(q-1)^3} \times (q^3 - q^2) \times (q^3 - q) \times (q^3 - 1) \\ &= \frac{q^3}{(q-1)^3} \times (q - 1) \times (q^2 - 1) \times (q^3 - 1) \end{aligned}$$

d'où

$$\begin{aligned} B_{3+j} &= \frac{q^3}{(q-1)^3} \times (q^{1+j}-1) \times (q^{2+j}-1) \times (q^{3+j}-1) \\ &= \frac{q^3}{(q-1)^3} \times A'_{3+j} \end{aligned}$$

$\lfloor \frac{3}{1} \rfloor = 3$ *donc* A'_{3+j} *est multiple de* $(q-1)^3$
$\lfloor \frac{3}{2} \rfloor = 1$ *donc* A'_{3+j} *est multiple de* (q^2-1)
$\lfloor \frac{3}{3} \rfloor = 1$ *donc* A'_{3+j} *est multiple de* (q^3-1)
donc A'_{3+j} *est multiple de* $A_3 = (q-1) \times (q^2-1) \times (q^3-1)$
on peut donc choisir $a_3 = \frac{q^3-1}{q-1}$ Plus généralement la récurrence permet de choisir à la k^{ieme} étape

$$a_k = \frac{q^k-1}{q-1} \quad \text{pour tout } k \in \mathbb{N}$$

donc $0, 1, \frac{q^2-1}{q-1}, ..., \frac{q^k-1}{q-1}, ...$ est un p-ordre de S''' pour tout p premier.

2/Prouvons que $k!_{S'''} = q^{\frac{k(k-1)}{2}} \times (q-1)^{-k} \times (q^k-1) \times (q^{k-1}-1) \times ..... \times (q-1)$.

$$\begin{aligned} k!_{S'''} &= (\frac{q^k-1}{q-1}-0) \times (\frac{q^k-1}{q-1}-1) \times (\frac{q^k-1}{q-1}-\frac{q^2-1}{q-1}) \times ..... \times (\frac{q^k-1}{q-1}-\frac{q^{k-1}-1}{q-1}) \\ &= (\frac{q^k-1}{q-1}) \times (\frac{q^k-q}{q-1}) \times (\frac{q^k-q^2}{q-1}) \times ..... \times (\frac{q^k-q^{k-1}}{q-1}) \\ &= \frac{1}{(q-1)^k} \times [(q^k-1) \times (q^k-q) \times (q^k-q^2) \times ..... \times (q^k-q^{k-1})] \\ &= (q-1)^{-k} \times [1 \times q \times q^2 \times ..... \times q^{k-1}] \times [(q^k-1) \times (q^{k-1}-1) \times ..... \times (q-1)] \\ &= q^{\frac{k(k-1)}{2}} \times (q-1)^{-k} \times (q^k-1) \times (q^{k-1}-1) \times ..... \times (q-1) \end{aligned}$$

•

9.2 Factorielles de Carlitz.

Un autre anneau naturel sur lequel s'applique la construction des factorielles est $\mathbb{F}_q[t]$, l'anneau des polynômes sur un corps fini de q éléments où q est premier.

Exemple 13 *Pour* $S = \mathbb{F}_q[t]$ *un t-ordre de S peut être construit comme suit :*
soit $a_0, a_1, ..., a_{q-1}$ *des éléments de* $\mathbb{F}_q$ *(avec* $a_0 = 0$*)*
et soit a_k *défini par :*

$$a_k = a_{c_0} + a_{c_1} t + ... + a_{c_h} t^h$$

où $\sum_{i=0}^{h} c_i q^i$ *est le développement de* k *dans la base* q.
On peut alors vérifier que ceci nous donne un P*-ordre de* $\mathbb{F}_q[t]$ *non seulement pour* $P = (t)$ *mais aussi pour tous les primitifs* $P \subset \mathbb{F}_q[t]$.
Il s'ensuit que :

$$k!_{\mathbb{F}_q[t]} = \prod_{i=1}^{h} (c_h)!_q \times (t^{q^h} - t)^{c_h} \times (t^{q^{h-1}} - t)^{c_{h-1} + c_h q} \times \ldots\ldots\ldots \times (t^q - t)^{c_1 + \ldots\ldots\ldots + c_h q^{h-1}}$$

où de nouveau $\sum_{i=0}^{h} c_i q^i$ *est le développement de* k *dans la base* q
et $(c_i!)$ *est donné modulo* q.

Remarque 8 *Il est noter que ici aussi* $\prod_{i=1}^{h} (c_h)!_q$ *n'apparaissait pas dans la formule donnée par M BHARGAVA.*

Preuve de l'exemple 13 :
1/Soit $\mathbb{F}_q[t]$ l'anneau des polynômes sur un corps fini de q éléments où q est premier.
Soit (pour $q \geq 2$)
$a_0 = 0,\ a_1 = 1, \ldots\ldots\ldots\ldots\ldots\ldots, a_{q-1} = q - 1$
$a_q = t,\ a_{q+1} = t + 1, \ldots\ldots\ldots\ldots, a_{2q-1} = t + q - 1$
$a_{2q} = 2t,\ a_{2q+1} = 2t + 1, \ldots\ldots\ldots, a_{3q-1} = 2t + q - 1$
$\vdots$
$a_{q^2} = t^2$.
On obtient les éléments de q ordonnés par leur représentation minimale dans $\mathbb{N}$.
Si $k = c_0 + c_1 q + \ldots\ldots\ldots + c_h q^h$ développement de k dans la base q alors $a_k = a_{c_0} + a_{c_1} t + \ldots\ldots\ldots + a_{c_h} t^h$.

exemple : $q = 5 \ \rightarrow\ \mathbb{Z}/5\mathbb{Z} = \{a_0 = 0,\ a_1 = 1,\ a_2 = 2,\ a_3 = 3,\ a_4 = 4\}$
alors on a :
$*\ a_0 = 0$
$*\ a_1 = 1$
$*\ a_2 = 2$
$*\ a_3 = 3 \equiv -2 \pmod 5$
$*\ a_4 = 4 \equiv -1 \pmod 5$
$5 = 0 \times 1 + 1 \times 5$ donc $c_0 = 0$ et $c_1 = 1$ donc $a_5 = a_0 + a_1 t$ d'où
$*\ a_5 = t$
$6 = 1 \times 1 + 1 \times 5$ donc $c_0 = 1$ et $c_1 = 1$ donc $a_6 = a_1 + a_1 t$ d'où
$*\ a_6 = 1 + t$
$7 = 2 \times 1 + 1 \times 5$ donc $c_0 = 2$ et $c_1 = 1$ donc $a_7 = a_2 + a_1 t$ d'où
$*\ a_7 = 2 + t$
$8 = 3 \times 1 + 1 \times 5$ donc $c_0 = 3$ et $c_1 = 1$ donc $a_8 = a_3 + a_t$ d'où
$*\ a_8 = 3 + t \equiv -2 + t \pmod 5$
$9 = 4 \times 1 + 2 \times 5$ donc $c_0 = 4$ et $c_1 = 1$ donc $a_9 = a_4 + a_t$ d'où

$*\ a_9 = 4 + t \equiv -1 + t \pmod 5$
$10 = 0 \times 1 + 2 \times 5$ donc $c_0 = 0$ et $c_1 = 2$ donc $a_10 = a_0 + a_2 t$ d'où
$*\ a_10 = 2t$
$11 = 1 \times 1 + 2 \times 5$ donc $c_0 = 1$ et $c_1 = 2$ donc $a_11 = a_1 + a_2 t$ d'où
$*\ a_11 = 1 + 2t$
$12 = 2 \times 1 + 2 \times 5$ donc $c_0 = 2$ et $c_1 = 2$ donc $a_12 = a_2 + a_2 t$ d'où
$*\ a_11 = 2 + 2t$
$13 = 3 \times 1 + 2 \times 5$ donc $c_0 = 3$ et $c_1 = 2$ donc $a_13 = a_3 + a_2 t$ d'où
$*\ a_13 = 3 + 2t \equiv -2 + 2t \pmod 5$
$14 = 4 \times 1 + 2 \times 5$ donc $c_0 = 4$ et $c_1 = 2$ donc $a_14 = a_4 + a_2 t$ d'où
$*\ a_14 = 4 + 2t \equiv -1 + 2t \pmod 5$
$\vdots$
on retrouve bien :
$a_0 = 0, \quad a_1 = 1, \quad a_2 = 2, \quad a_3 = 3, \quad a_{q-1} = a_4 = q - 1 = 4$

$a_q = a_5 = t, \quad a_{q+1} = a_6 = t + 1, \quad a_{q+2} = a_7 = t + 2,$
$a_{q+3} = a_8 = t + 3, \quad a_{2q-1} = a_9 = t + q - 1 = t + 4$

$a_{2q} = a_{10} = 2t, \quad a_{2q+1} = a_{11} = 2t + 1, \quad a_{2q+2} = a_{12} = 2t + 2,$
$a_{2q+3} = a_{13} = 2t + 3, \quad a_{3q-1} = a_{14} = 2t + q - 1 = 2t + 4$
$\vdots$

Montrons que la suite ainsi construite est un t-ordre et plus généralement un P-ordre où $P(t)$ est un polynôme primitif.
$*$ Si $k \leq q - 1 \quad w_t[(a_k - a_0) \times (a_k - a_1) \times ..... \times (a_k - a_{k-1})] = t^0 = 1$ (ou $w_P = [P(t)]^0$ plus généralement).
$*$ Si $k = q \qquad w_t[(a_k - a_0) \times (a_k - a_1) \times ..... \times (a_k - a_{k-1})] = t$ si $\mathrm{d}^\circ a_k = 1$.
$*$ Si $q < k < 2q \quad w_t[(a_k - a_0) \times (a_k - a_1) \times ..... \times (a_k - a_{k-1})] = t$ si $a_k = t + \alpha \ \ (0 < \alpha < q - 1)$.

exemple : $q = 5$
$*$ *Si* $k = 4 \leq q - 1$

$$\begin{aligned} w_t[(a_4 - a_0) \times (a_4 - a_1) \times (a_4 - a_2) \times (a_4 - a_3)] &= w_t[-3 \times -2 \times -1 \times 1] \\ &= w_t[6] \\ &= t^0 \\ &= 1 \end{aligned}$$

$*$ *Si* $k = 5$

$w_t[(a_5 - a_0) \times (a_5 - a_1) \times (a_5 - a_2) \times (a_5 - a_3) \times (a_5 - a_4)]$
$= w_t[t \times (t - 1) \times (t - 2) \times (t + 2) \times (t + 1)]$

$= t$

$*$ *Si* $5 < k = 6 < 10$

$w_t[(a_6 - a_0) \times (a_6 - a_1) \times (a_6 - a_2) \times (a_6 - a_3) \times (a_6 - a_4) \times (a_6 - a_5)]$
$= w_t[(t+1) \times t \times (t-1) \times (t-2) \times (t+2) \times 1]$
$= t$

De façon générale pour minimiser $w_t[\ ]$ au rang $k+1$, si $w_t[\ ]$ est un minimum au rang k, il suffit de minimiser le degré de $a_{k+1} - a_k$ ce qui justifie la construction choisie du t-ordre.
La suite est également un P-ordre si P est un polynôme primitif.

exemple : $q = 5$ *et* $P(t) = 1 + t$
seul le choix de $a_5 = t$ *donne* $w_t[\ ] = P^0 = 1$.
Puis pour a_6 *tout choix donnerait* $w_P[\ ] \geq 1$ *ce qui permet le choix de* $a_6 = P(t) = 1 + t$
La suite construite donne $w_P[\ ] = P^1$ *jusqu'à* $k = 11$ *et* $w_P[\ ] \geq P^2$ *pour un polynôme n'appartenant pas à* $a_0, a_1, ..., a_{11}$ *etc...*

2/Calcul de $k!_{\mathbb{F}_q[t]}$.

Pour q quelconque la construction rend évident le résultat suivant :
$*$ $k \leq q-1 \qquad k!_{\mathbb{F}_q[t]} = (k!)_q = (a_{c_0}!)_q$ où $(k!)_q$ désigne la valeur modulo q de $k!$.

exemple : $q = 5$
$*$ $k = 1$

$$1!_{\mathbb{F}_q[t]} = 1$$

$*$ $k = 2$

$$2!_{\mathbb{F}_{q[t]}} = 2$$

$*$ $k = 3$ *et* $a_{c_0} = 3$

$$\begin{aligned} 3!_{\mathbb{F}_q[t]} &= (3-0) \times (3-1) \times (3-2) \\ &= 3 \times 2 \times 1 \\ &= 6 \\ &\equiv 1 \pmod 5 \\ &= (3!)_5 \end{aligned}$$

$*$ $k = 4$ *et* $a_{c_0} = 4$

$$\begin{aligned} 4!_{\mathbb{F}_q[t]} &= (4-0) \times (4-1) \times (4-2) \times (4-3) \\ &= 4 \times 3 \times 2 \times 1 \\ &= 24 \\ &\equiv 4 \pmod 5 \\ &= (4!)_5 \end{aligned}$$

$*$ si $k \geq q$ on obtient plus généralement

$$k!_{\mathbb{F}_q[t]} = \prod_{i=0}^{k} (c_i!)_q \times (t^{q^h} - t)^{c_h} \times (t^{q^{h-1}} - t)^{c_{h-1} + c_h q} \times \ldots\ldots\ldots \times (t^q - t)^{c_1 + \ldots\ldots\ldots + c_h q^{h-1}}$$

où de nouveau $\sum_{i=0}^{h} c_i q^i$ est le développement de k dans la base q
et $(c_i!)$ est donné modulo q.
Ce qui peut s'obtenir en montrant

$$(a_{c_0} + \sum_{i=0}^{h} a_{c_h} t^h)!_{\mathbb{F}_q[t]} = (a_{c_0}!)q \times (\sum_{i=1}^{h} a_{c_h} t^h)!_{\mathbb{F}_q[t]}$$

exemple : $q = 5$
$(11!)_{\mathbb{F}_q[t]} = (10!)_{\mathbb{F}_q[t]}$
$(12!)_{\mathbb{F}_q[t]} = (2!)_{\mathbb{F}_q[t]} (10!)_{\mathbb{F}_q[t]}$
$(13!)_{\mathbb{F}_q[t]} = (3!)_{\mathbb{F}_q[t]} (10!)_{\mathbb{F}_q[t]}$
$(14!)_{\mathbb{F}_q[t]} = (4!)_{\mathbb{F}_q[t]} (10!)_{\mathbb{F}_q[t]}$
puis $(k+5)!_{\mathbb{F}_q[t]} = (c_1)_q \times (t^5 - t) \times (k!)_{\mathbb{F}_q[t]}$
ce qui nous donne par exemple :
$40 = 0 \times 1 + 13 \times 5 + 1 \times 5^2$ *donc* $c_0 = 0$, $c_1 = 3$ *et* $c_2 = 1$
d'où

$$\begin{aligned} (40!)_{\mathbb{F}_q[t]} &= (3)_5 \times (t^5 - t) \times (35!)_{\mathbb{F}_q[t]} \\ &= (3 \times 2)_5 \times (t^5 - t) \times (30!)_{\mathbb{F}_q[t]} \qquad car\ 35 = 0 \times 1 + 2 \times 5 + 1 \times 5^2\ donc\ c_1 = 2 \\ &= (6)_5 \times (t^5 - t) \times (25!)_{\mathbb{F}_q[t]} \\ &= (t^5 - t) \times (25!)_{\mathbb{F}_q[t]} \end{aligned}$$

La généralisation de tels résultats aux (c_i) pour i de 1 à h permet d'obtenir $k!_{\mathbb{F}_q[t]}$ où apparaissent les factorielles de CARLITZ.

Chapitre 10

QUESTIONS DE COMBINATOIRE ET D'ANALYSE LIEES AUX FACTORIELLES GENERALISEES.

Les factorielles généralisées, étudiées précédemment dans ce travail,sont certainement la bonne généralisation des fonctions factorielles pour des sous-ensembles de $\mathbb{Z}$.
Quel sens pourrait avoir l'analyse combinatoire avec cette généralisation ?

10.1 $k!_S$ en combinatoire.

Question 1 *Pour $S \subset \mathbb{Z}$, comment interpréter $k!_S$ en combinatoire ?*

Une interprétation parait assez naturelle dans le cas d'un sous ensemble S pour lequel un p-ordre peut être défini pour tout p premier.
En effet, dans ce cas

$$n!_S = (a_n - a_0) \times (a_n - a_1) \times ..... \times (a_n - a_{n-1})$$

alors $n!_S$ peut être défini comme le nombre d'applications de $[|1; n|]$ vers $\mathbb{Z}$ telle que :
1 ait son image dans $[|1; a_n - a_0|]$
$\vdots$
k ait son image dans $[|1; a_n - a_{k-1}|]$
$\vdots$

n ait son image dans $[|1; a_n - a_{n-1}|]$.

Donnons trois exemples d'interprétation combinatoire de $k!_S$ à partir des exemples 6, 7 et 8.

Exemple 14 *Dans l'ensemble des entiers pairs $(n!)_{2\mathbb{Z}}$ est le nombre d'applications injectives de $[|1; n|]$ vers $[|-n; n|]^*$ telles que x et y distincts ne puissent avoir une image égale en valeur absolue.*

exemple :
si $n = 3$ alors

$$\begin{aligned}(3!)_{2\mathbb{Z}} &= 2^3 \times 3! \\ &= 8 \times 3 \times 2 \times 1 \\ &= 48\end{aligned}$$

ce qui équivaut bien à

$$123 \rightarrow 8 \begin{cases} \overbrace{\begin{array}{cccccc} 123 & 132 & 213 & 231 & 312 & 321 \end{array}}^{6} \\ 1-23 \\ 1-23 \\ 12-3 \\ -1-23 \\ -12-3 \\ 1-2-3 \\ -1-2-3 \end{cases}$$

soit $8 \times 6 = 48 = (3!)_{2\mathbb{Z}}$ applications injectives de $[|1; 3|]$ vers $[|-3; 3|]^*$ telles que x et y distincts ne puissent avoir une image égale en valeur absolue.

Exemple 15 *Dans l'ensemble des puissances de 2 dans $\mathbb{Z}$, $(n!)_S$ est le nombre d'applications de $[|1; n|]$ vers $\mathbb{Z}$ telles que $k \in [|1; n|]$ ait son image dans $\left[\left|1; 2^n - 2^{k-1}\right|\right]$.*

exemple :
si $n = 3$ alors

$$\begin{aligned}(3!)_S &= (2^3 - 1) \times (2^3 - 2) \times (2^3 - 2^2) \\ &= 7 \times 6 \times 4\end{aligned}$$

ce qui équivaut bien à
$k = 1$ a son image dans $\left[\left|1; 2^3 - 2^0\right|\right] = \{1, 2, 3, 4, 5, 6, 7\}$
$k = 2$ a son image dans $\left[\left|1; 2^3 - 2^1\right|\right] = \{1, 2, 3, 4, 5, 6\}$
$k = 3$ a son image dans $\left[\left|1; 2^3 - 2^2\right|\right] = \{1, 2, 3, 4\}$
soit $7 \times 6 \times 4 = (3!)_S$ applications de $[|1; 3|]$ vers $\mathbb{Z}$ telles que $k \in [|1; 3|]$ ait son image dans $\left[\left|1; 2^3 - 2^{k-1}\right|\right]$.

Exemple 16 *Dans l'ensemble des carrés de $\mathbb{Z}$, $(n!)_{S'}$ est le nombre d'applications de $[|1;n|]$ vers $\mathbb{Z}$ telles que $k \in [|1;n|]$ ait son image dans $\left[\left|1;n^2-k-1^2\right|\right]$.*

exemple :
si $n=3$ alors

$$\begin{aligned}(3!)_{S'} &= 3^2 \times (3^2-1^2) \times (3^2-2^2) \\ &= 9 \times 8 \times 5\end{aligned}$$

ce qui équivaut bien à
$k=1$ a son image dans $\left[\left|1;9-0^2\right|\right] = [|1;9|]$
$k=2$ a son image dans $\left[\left|1;9-1^2\right|\right] = [|1;8|]$
$k=3$ a son image dans $\left[\left|1;9-2^2\right|\right] = [|1;5|]$
soit $9 \times 8 \times 5 = (3!)_{S'}$ applications de $[|1;3|]$ vers $\mathbb{Z}$ telles que $k \in [|1;3|]$ ait son image dans $\left[\left|1;9-k-1^2\right|\right]$.

10.2 $(C_n^k)_S$ en combinatoire.

Question 2 *Pour $S \subset \mathbb{Z}$, comment interpréter $(C_n^k)_S$ en combinatoire ?*

Donnons trois exemples d'interprétation combinatoire de $k!_S$ à partir des exemples 6, 7 et 8.

Exemple 17 *Dans l'ensemble des entiers pairs*

$$\begin{aligned}(C_n^k)_{2\mathbb{Z}} &= \frac{(n!)_{2\mathbb{Z}}}{(k!)_{2\mathbb{Z}} \times (n-k)!_{2\mathbb{Z}}} \\ &= \frac{2^n \times n!}{2^k \times k! \times 2^{n-k} \times (n-k)!} \\ &= \frac{2^n}{2^k \times 2^{n-k}} \times \frac{n!}{k! \times (n-k)!} \\ &= \frac{n!}{k! \times (n-k)!} \\ &= C_n^k\end{aligned}$$

Lorsque $(A_n^k)_S$ peut être interprété comme le nombre de certaines applications de $[|1;n|]$ vers $\mathbb{Z}$, $(C_n^k)_S$ est alors défini comme dans $\mathbb{Z}$ par $(C_n^k)_S = \frac{(A_n^k)_S}{(k!)_S}$.
Remarquons que $(A_n^n)_S = n!$

Exemple 18 *Dans l'ensemble des puissances de 2 dans $\mathbb{Z}$, $(n!)_S$, on définit $(A_n^k)_S = \frac{(n!)_S}{(n-k)!_S}$ comme le nombre d'applications de $[|1;n|]$ vers $\mathbb{Z}$ telles que*
si $i \leq k$, i ait son image dans $\left[\left|1;2^n-2^{i-1}\right|\right]$
si $i > k$, i ait son image dans $\left[\left|1;2^k\right|\right]$.

exemple :
si $n = 6$ *et* $k = 3$ *alors*

$$\begin{aligned}(A_3^6)_S &= \frac{(6!)_S}{(3!)_S} \\ &= \frac{(2^6-1)(2^6-2)(2^6-2^2)(2^6-2^3)(2^6-2^4)(2^6-2^5)}{(2^3-1)(2^3-2)(2^3-2^2)} \\ &= \frac{63\times 62\times 60\times 56\times 48\times 32}{7\times 6\times 4} \\ &= 63\times 62\times 60\times \frac{56}{7}\times\frac{48}{6}\times\frac{32}{4} \\ &= 63\times 62\times 60\times 8^3\end{aligned}$$

ce qui équivaut bien à
$i = 1$ *a son image dans* $\left[\left|1; 2^6-2^0\right|\right] = [|1;63|]$
$i = 2$ *a son image dans* $\left[\left|1; 2^6-2^1\right|\right] = [|1;62|]$
$i = 3$ *a son image dans* $\left[\left|1; 2^6-2^2\right|\right] = [|1;60|]$
$i = 4$ *a son image dans* $[|1;8|]$
$i = 5$ *a son image dans* $[|1;8|]$
$i = 6$ *a son image dans* $[|1;8|]$
soit $63\times 62\times 60\times 8^3 = (A_3^6)_S$ *applications de* $[|1;6|]$ *vers* $\mathbb{Z}$ *telles que*
si $i \leq 3$, i *ait son image dans* $\left[\left|1; 2^6-2^{i-1}\right|\right] = \left[\left|1; 64-2^{i-1}\right|\right]$
si $i > 3$, i *ait son image dans* $\left[\left|1; 2^3\right|\right] = [|1;8|]$.
et

$$\begin{aligned}(C_3^6)_S &= \frac{(A_3^6)_S}{(3!)_S} \\ &= \frac{63\times 62\times 60\times 8^3}{7\times 6\times 4}\end{aligned}$$

Exemple 19 *Dans l'ensemble des carrés de* $\mathbb{Z}$

$$\begin{aligned}(C_n^k)_{S'} &= \frac{(n!)_{S'}}{(k!)_{S'}\times(n-k)!_{S'}} \\ &= \frac{\frac{(2n)!}{2}}{\frac{(2k)!}{2}\times\frac{(2\times(n-k))!}{2}} \\ &= \frac{(2n)!}{2}\times\frac{4}{(2k)!\times(2\times(n-k))!} \\ &= 2C_{2n}^{2k}\end{aligned}$$

Question 3 *Peut-on évoquer les fonctions factorielles et la combinatoire sans évoquer le binôme de NEWTON*

$$(a+b)^n = \sum_{k=0}^{\infty} C_n^k \times a^k \times b^{n-k}$$

et le triangle de PASCAL

$$\begin{array}{ccccc} 1 & & & & \\ 1 & 1 & & & \\ 1 & 2 & 1 & & \\ 1 & 3 & 3 & 1 & \\ 1 & 4 & 6 & 4 & 1 \end{array}$$

Que donneraient NEWTON et PASCAL avec les factorielles généralisées ?

Voici, en tout cas, des débuts de quelques triangles :

Exemple 20 *Dans l'ensemble des entiers pairs, on a vu que*

$$(C_n^k)_{2\mathbb{Z}} = C_n^k$$

donc le triangle est identique au triangle de PASCAL.

Exemple 21 *Dans l'ensemble des puissances de 2 dans $\mathbb{Z}$, on a vu que*

$$(n!)_S = (2^n-1) \times (2^n-2) \times (2^n-2^2) \times ..... \times (2^n-2^{n-1})$$

et

$$(C_n^k)_S = \frac{(2^n-1) \times ..... \times (2^n-2^{n-1})}{(2^{n-k}-1) \times ..... \times (2^{n-k}-2^{n-k-1}) \times (2^k-1) \times ..... \times (2^k-2^{k-1})}$$

ce qui nous donne :

$(C_2^1)_S = \frac{(2^2-1)\times(2^2-2)}{(2-1)\times(2-1)} = 6$

$(C_3^1)_S = \frac{(2^3-1)\times(2^3-2)\times(2^3-2^2)}{(2^2-1)\times(2^2-2)\times(2-1)} = \frac{168}{6} = 28$

$(C_3^2)_S = \frac{(2^3-1)\times(2^3-2)\times(2^3-2^2)}{(2-1)\times(2^2-1)\times(2^2-2)} = \frac{168}{6} = 28$

$(C_4^1)_S = \frac{(2^4-1)\times(2^4-2)\times(2^4-2^2)\times(2^4-2^3)}{(2^3-1)\times(2^3-2)\times(2^3-2^2)\times(2-1)} = \frac{20160}{168} = 120$

$(C_4^2)_S = \frac{(2^4-1)\times(2^4-2)\times(2^4-2^2)\times(2^4-2^3)}{(2^2-1)\times(2^2-2)\times(2^2-1)\times(2^2-2)} = \frac{20160}{36} = 560$

$(C_4^3)_S = \frac{(2^4-1)\times(2^4-2)\times(2^4-2^2)\times(2^4-2^3)}{(2-1)\times(2^3-1)\times(2^3-2)\times(2^3-2^2)} = \frac{20160}{168} = 120$

d'où on en déduit le triangle suivant :

$$\begin{array}{ccccc} 1 & & & & \\ 1 & 1 & & & \\ 1 & 6 & 1 & & \\ 1 & 28 & 28 & 1 & \\ 1 & 120 & 560 & 120 & 1 \end{array}$$

Exemple 22 *Dans l'ensemble des carrés de* $\mathbb{Z}$*, on a vu que*

$$(n!)_{S'} = \frac{(2n)!}{2}$$

et

$$(C_n^k)_{S'} = 2C_{2n}^{2k}$$

d'où on en déduit le triangle suivant :

$$\begin{array}{ccccc} 1 & & & & \\ 1 & 1 & & & \\ 1 & 12 & 1 & & \\ 1 & 30 & 30 & 1 & \\ 1 & 56 & 140 & 56 & 1 \end{array}$$

Exemple 23 *Dans l'ensemble des premiers de* $\mathbb{Z}$*, on a vu que*

$$(n!)_{S''} = \prod_{p,\ p\ premier} p^{\left\lfloor \frac{n-1}{p-1} \right\rfloor + \left\lfloor \frac{n-1}{p(p-1)} \right\rfloor + \left\lfloor \frac{n-1}{p^2(p-1)} \right\rfloor + \cdots\cdots\cdots}$$

et

$$(C_n^k)_{S''} = \frac{\prod_{p,\ p\ premier} p^{\left\lfloor \frac{n-1}{p-1} \right\rfloor + \left\lfloor \frac{n-1}{p(p-1)} \right\rfloor + \left\lfloor \frac{n-1}{p^2(p-1)} \right\rfloor + \cdots}}{\prod_{p,\ p\ premier} p^{\left\lfloor \frac{n-k-1}{p-1} \right\rfloor + \left\lfloor \frac{n-k-1}{p(p-1)} \right\rfloor + \left\lfloor \frac{n-k-1}{p^2(p-1)} \right\rfloor + \cdots} \times \prod_{p,\ p\ premier} p^{\left\lfloor \frac{n-1}{p-1} \right\rfloor + \left\lfloor \frac{n-1}{p(p-1)} \right\rfloor + \left\lfloor \frac{n-1}{p^2(p-1)} \right\rfloor + \cdots}}$$

d'où on en déduit le triangle suivant :

$$\begin{array}{ccccc} 1 & & & & \\ 1 & 1 & & & \\ 1 & 2 & 1 & & \\ 1 & 12 & 12 & 1 & \\ 1 & 2 & 12 & 2 & 1 \end{array}$$

Exemple 24 *Pour les factoriels de CARLITZ , on a avec* $q = 3$

$a_0 = 0 \qquad a_1 = 1 \qquad a_2 = -1$

$a_3 = t \qquad a_4 = t + 1 \quad a_5 = t - 1$

et

$0! = 1$

$1! = 1$

$2! = 2$

$3! = t^3 - t$

$4! = t^3 - t$

d'où on en déduit le triangle suivant :

$$\begin{array}{ccccc} 1 & & & & \\ 1 & 1 & & & \\ 1 & 2 & 1 & & \\ 1 & \frac{t^3-t}{2} & \frac{t^3-t}{2} & 1 & \\ 1 & 1 & \frac{t^3-t}{4} & 1 & 1 \end{array}$$

10.3 La fonction Gamma.

Question 4 *Pour $S \subset \mathbb{Z}$, y a t-il des interpolations analytiques naturelles complexes de $k!_S$ pour généraliser les fonctions Γ_S ?*

On sait que la fonction factorielle a une extension naturelle vers une fonction continue sur $\mathbb{R}^+$ appelée fonction GAMMA, et définie par

$$\Gamma(x+1) = \int_{\infty}^{0} e^{-t} \times t^x \; dt$$

et cette fonction GAMMA peut avoir un prolongement méromorphe sur tout le plan complexe.
En effet :

$$\begin{aligned} \Gamma(n+1) &= \int_{\infty}^{0} e^{-t} \times t^n \; dt \\ &= \left[-e^{-t} \times t^n\right]_0^{\infty} + n \times \int_{\infty}^{0} e^{-t} \times t^{n+1} \; dt \\ &= n \times \Gamma(n) \end{aligned}$$

On en déduit par récurrence que

$$\Gamma(n+1) = n!$$

car

$$\begin{aligned} \Gamma(0) &= \int_{\infty}^{0} e^{-t} \; dt \\ &= \left[-e^{-t}\right]_0^{\infty} \\ &= 1 \end{aligned}$$

Donnons deux exemples des fonctions Γ_S à partir des exemples 6 et 8.

Exemple 25 *Dans l'ensemble des entiers pairs en définissant*

$$\Gamma_{2\mathbb{Z}}(n+1) = \int_{\infty}^{0} e^{-t} \times (2t)^n \; dt$$

on obtient :

$$\begin{aligned} \Gamma_{2\mathbb{Z}}(n+1) &= 2^n \times \int_{\infty}^{0} e^{-t} \times t^n \; dt \\ &= 2^n \times \Gamma(n+1) \\ &= 2^n \times n! \\ &= (n!)_{2\mathbb{Z}} \end{aligned}$$

Exemple 26 *Dans l'ensemble des carrés de $\mathbb{Z}$ en définissant*

$$\Gamma_{S'}(n+1) = \int_{\infty}^{0} \frac{1}{2} \times e^{-t} \times (t^2)^n \ dt$$

on obtient :

$$\begin{aligned} \Gamma_{S'}(n+1) &= \frac{1}{2} \times \int_{\infty}^{0} e^{-t} \times t^{2n} \ dt \\ &= \frac{1}{2} \times \Gamma(n+1) \\ &= \frac{(2n)!}{2} \\ &= (n!)_{S'} \end{aligned}$$

Pour ces deux exemples, une extension à $\mathbb{R}^+$ et à $\mathbb{C}$ analogue à l'extension pour la fonction GAMMA usuelle semble assez naturelle.

10.4 La formule de Stirling.

Question 5 *Les fonctions factorielles généralisées peuvent-elles admettre des formules analogues à la formule de STIRLING ?*

Dans $\mathbb{Z}$ la formule de STIRLING peut s'écrire

$$n! = \left(\frac{n}{e}\right)^n \times \sqrt{2\pi n} \times (1+\epsilon_n) \quad \text{avec } \lim_{n\to\infty} \epsilon_n = 0$$

ce qui donne un infiniment grand équivalent à $n!$.
Voici une brève démonstration de cette formule :
Posons

$$n! = \left(\frac{n}{e}\right)^n \times \sqrt{n} \times f(n)$$

alors

$$\begin{aligned} \frac{f(n+1)}{f(n)} &= \frac{(n+1)!_{2\mathbb{Z}}}{n!_{2\mathbb{Z}}} \times e \times \frac{(2n)^n \times \sqrt{n}}{(2(n+1))^{n+1} \times \sqrt{n+1}} \\ &= 2(n+1) \times e \times \frac{2^n \times n^{n+\frac{1}{2}}}{2^{n+1} \times (n+1)^{n+\frac{3}{2}}} \\ &= \left(\frac{n}{n+1}\right)^{n+\frac{1}{2}} \times e \end{aligned}$$

Posons

$$u_n = ln\ f(n+1) - ln\ f(n)$$

en montrant que u_n est une suite convergente, on prouve que $lim_{n\to\infty} f(n) = \sqrt{2\pi}$ et la formule de STIRLING s'ensuit.

Donnons deux formules analogues à partir des exemples 6 et 8.

Exemple 27 *Dans l'ensemble des entiers pairs en définissant*

$$n!_{2\mathbb{Z}} = \left(\frac{2n}{e}\right)^n \times \sqrt{n} \times g(n)$$

on obtient :

$$\begin{aligned}
\frac{g(n+1)}{g(n)} &= \frac{(n+1)!_{2\mathbb{Z}}}{n!_{2\mathbb{Z}}} \times e \times \frac{(2n)^n}{(2(n+1))^{n+1}} \times \frac{\sqrt{n}}{\sqrt{n+1}} \\
&= 2(n+1) \times e \times \frac{2^n \times n^{n+\frac{1}{2}}}{2^{n+1} \times (n+1)^{n+\frac{3}{2}}} \\
&= e \times \left(\frac{n}{n+1}\right)^{n+\frac{1}{2}} \\
&= \frac{f(n+1)}{f(n)}
\end{aligned}$$

donc, comme pour f, on montre $lim_{n\to\infty} g(n) = \sqrt{2\pi}$ et on peut ainsi définir un infiniment grand équivalent à $(n!)_{2\mathbb{Z}}$ soit

$$(n!)_{2\mathbb{Z}} = \left(\frac{2n}{e}\right)^n \times \sqrt{2\pi n} \times (1+\epsilon_n) \quad \textit{avec } lim_{n\to\infty}\epsilon_n = 0$$

Exemple 28 *Dans l'ensemble des carrés de $\mathbb{Z}$ une formule analogue a la formule de STIRLING peut être :*

$$(n!)_{S'} = lim_{n\to\infty} \left(\frac{2n}{e}\right)^{2n} \times \sqrt{\pi n}$$

puisque $lim_{n\to\infty} \left(\frac{2n}{e}\right)^{2n} \times \frac{1}{2} \times \sqrt{2\pi 2n} = \frac{1}{2}(2n)!$

10.5 La fonction exponentielle.

Question 6 *Peut-on trouver dans S une fonction analogue a la fonction exponentielle ?*

On sait que dans $\mathbb{Z}$, $e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$ pour $x \in \mathbb{R}$ et $k \in \mathbb{N}$.
Donnons deux exemples des fonctions exponentielles à partir des exemples 6 et 8.

Exemple 29 *Dans l'ensemble des entiers pairs en définissant*

$$(e^x)_{2\mathbb{Z}} = \sum_{k=0}^{\infty} \frac{x^k}{(k!)_{2\mathbb{Z}}}$$

on obtient :

$$\begin{aligned}(e^x)_{2\mathbb{Z}} &= \sum_{k=0}^{\infty} \frac{x^k}{2^k \times k!} \\ &= \sum_{k=0}^{\infty} \frac{(\frac{x}{2})^k}{k!} \\ &= e^{\frac{x}{2}}\end{aligned}$$

On peut généraliser ce résultat pour l'ensemble $a\mathbb{Z}+b$ (c'est à dire les entiers égaux à b modulo a),
en effet, en définissant

$$(e^x)_{a\mathbb{Z}+b} = \sum_{k=0}^{\infty} \frac{x^k}{(k!)_{a\mathbb{Z}+b}}$$

on obtient :

$$\begin{aligned}(e^x)_{a\mathbb{Z}+b} &= \sum_{k=0}^{\infty} \frac{x^k}{a^k \times k!} \\ &= \sum_{k=0}^{\infty} \frac{(\frac{x}{a})^k}{k!} \\ &= e^{\frac{x}{a}}\end{aligned}$$

Exemple 30 *Dans l'ensemble des carrés de $\mathbb{Z}$ en définissant*

$$(e^x)_{S'} = \sum_{k=0}^{\infty} \frac{x^k}{(k!)_{S'}}$$

on obtient :

$$\begin{aligned}(e^x)_{S'} &= \sum_{k=0}^{\infty} \frac{x^k}{\frac{(2k)!}{2}} \\ &= 2\sum_{k=0}^{\infty} \frac{x^k}{(2k)!} \\ &= 2[1 + \frac{x}{2!} + \frac{x^2}{4!} + ...] \\ &= 2 \times \frac{e^{\sqrt{x}} + e^{-\sqrt{x}}}{2} \\ &= e^{\sqrt{x}} + e^{-\sqrt{x}}\end{aligned}$$

Chapitre 11

CONCLUSION.

La fonction factorielle usuelle intervient dans différents domaines tels que problèmes d'arithmétique (chapitre 1 :théorèmes 2, 3, 4 et 6) et résultats sur les polynômes, la fonction Gamma, la formule de Stirling et la fonction exponentielle.
Ces résultats importants peuvent-ils tous rester vrais lorsqu'on remplace $\mathbb{Z}$ par un sous-ensemble S de $\mathbb{Z}$ ou d'un anneau de Dedekind ?
Les notions de p-ordre et de factorielle généralisée (chapitre 3) permettent de répondre par l'affirmative à cette question (chapitre 4 :théorèmes 8, 9, 10 et 11, chapitre 6 et chapitre 12).Elles étendent également les résultats d'arithmétique à un sous ensemble S de $\mathbb{Z}^n$ où $n \geq 1$ (chapitre 7).
Mais les questions posées par ces généralisations n'ont probablement pas toutes reçues de réponses à ce jour, par exemple :
∘ comment généraliser le binôme de Newton et le triangle de Pascal dans S ?
∘ ou bien quels sont les sous-ensembles d'un anneau d'entiers, dans un corps de nombres ou un corps de fonctions, qui admettent un p-ordre simultanément pour tout premier p ?

Chapitre 12

BIBLIOGRAPHIE.

⊗ 'The factorial function and generalizations' paru en novembre 2000 dans 'The mathematical association of America' pages 783 à 798.

⊗ 'Algèbre commutative', R GLOBOT, DUNOT.