

# UN THÉORÈME MÉCONNU DE BURNSIDE SUR LES SOUS-GROUPES D'INDICE PREMIER

Le joli résultat qui suit, connu a priori des seuls spécialistes de la théorie des groupes finis, date de 1901. Burnside l'a démontré à l'époque avec les outils naissants de la théorie des caractères, mais Schur en a donné peu après une preuve élémentaire en termes de corps finis et c'est une preuve de ce genre que nous étudierons.

■ **Théorème 1** Tout groupe fini simple non abélien qui possède un sous-groupe d'indice premier est d'ordre pair.

À l'époque, ce théorème accréditait l'idée que tout groupe fini simple non abélien est d'ordre pair — un résultat TRÈS difficile de 1963 que nous appelons aujourd'hui le *théorème de Feit-Thompson*. En réalité, cela dit, Burnside a prouvé mieux que le théorème 1 et c'est à la démonstration du théorème qui suit que nous allons vraiment nous attaquer. Nous verrons assez vite que le théorème 1 en découle trivialement. — Pour celles et ceux qui ne seraient pas familiers avec ce concept, la *2-transitivité* sera définie proprement dans une première partie de préliminaires.

■ **Théorème 2 (Sous-groupes transitifs de  $S_p$ , un théorème de Burnside)** Soit  $p$  un nombre premier. Tout sous-groupe transitif du groupe symétrique  $S_p$  est :

- soit 2-transitif,
- soit isomorphe à un sous-groupe du groupe affine  $GA(\mathbb{F}_p) = \{x \mapsto ax+b \mid a \in \mathbb{F}_p^* \text{ et } b \in \mathbb{F}_p\}$ . En particulier, dans ce cas,  $G$  est résoluble.

La structure du groupe affine  $GA(\mathbb{F}_p)$  est facile à décrire. L'action de  $\mathbb{F}_p^*$  sur  $\mathbb{F}_p$  par simple multiplication définit en effet un produit semi-direct  $\mathbb{F}_p \rtimes \mathbb{F}_p^*$  auquel  $GA(\mathbb{F}_p)$  est isomorphe via l'application  $(a, b) \mapsto (x \mapsto ax + b)$ . Le groupe affine  $GA(\mathbb{F}_p)$  est ainsi résoluble en tant que produit semi-direct de deux groupes abéliens.

La classification des groupes finis simples a permis d'atteindre de bien meilleurs résultats — mais à quel prix ! — dont par exemple le théorème suivant que Guralnick a démontré en 1981.

■ **Théorème (Sous-groupes transitifs simples non abéliens de  $S_{p^n}$ )** Soient  $p$  un nombre premier,  $n \in \mathbb{N}^*$  et  $G$  un sous-groupe transitif de  $S_{p^n}$  simple non abélien. Alors  $G$  est 2-transitif, sauf si  $p = n = 3$  et  $|G| = 25920$  — auquel cas  $G$  est isomorphe à un certain  $PSU_4(\mathbb{F}_2)$ .

Avant de démontrer le théorème de Burnside 2, on peut citer sans preuve deux familles classiques de groupes finis simples non abéliens qui possèdent un sous-groupe d'indice premier. D'après la classification des groupes finis simples, d'ailleurs, seuls deux autres groupes finis simples non abéliens possèdent cette propriété — les groupes de Mathieu  $M_{11}$  et  $M_{23}$ .

**Exemple** Pour tout nombre premier  $p$  supérieur ou égal à 5, le groupe  $A_p$  est simple, le sous-groupe  $A_{p-1}$  est d'indice  $p$  dans  $A_p$ , et bien sûr  $A_p$  est 2-transitif sur  $\llbracket 1, p \rrbracket$ .

**Exemple** Soient  $q$  une puissance non triviale d'un nombre premier et  $n \geq 2$ .

- Le groupe spécial linéaire  $PSL_n(\mathbb{F}_q)$  est simple sauf si  $(q, n) \in \{(2, 2), (3, 2)\}$ .
- Pour tous vecteurs  $x, y, x', y' \in \mathbb{F}_q^n \setminus \{(0, \dots, 0)\}$ , si les familles  $(x, y)$  et  $(x', y')$  sont libres, il existe une matrice  $M \in GL_n(\mathbb{F}_q)$  pour laquelle  $x' = Mx$  et  $y' = My$ . Si de plus  $n \geq 3$ , on peut même imposer à  $M$  d'appartenir à  $SL_n(\mathbb{F}_q)$ . En d'autres termes, si  $n \geq 3$ , le groupe  $SL_n(\mathbb{F}_q)$  — mais donc aussi  $PSL_n(\mathbb{F}_q)$  — est 2-transitif sur l'ensemble des droites vectorielles de  $\mathbb{F}_q^n$ , de cardinal  $\frac{q^n - 1}{q - 1}$ . L'entier  $\frac{q^n - 1}{q - 1}$  est-il cependant un nombre premier ? En général non, mais parfois oui — et dans ce cas,  $n$  est premier. C'est par exemple le cas des couples  $(q, n)$  suivants :

$$(2, 2), (2, 3), (2, 5), (2, 7), (2, 13), (2, 17), (2, 19) \dots, \quad (3, 3), (3, 7), (3, 13) \dots,$$

$$(5, 3), (5, 7), (5, 11), (5, 13) \dots, \quad (7, 5), (7, 13) \dots, \quad (11, 17), (11, 19) \dots, \quad (13, 5), (13, 7) \dots$$

- Plus explicitement, tout stabilisateur de droite vectorielle est un exemple de sous-groupe d'indice  $\frac{q^n - 1}{q - 1}$  de  $\text{PSL}_n(\mathbb{F}_q)$ . Le stabilisateur dans  $\text{SL}_n(\mathbb{F}_q)$  de la droite vectorielle engendrée par  $(1, 0, \dots, 0)$  coïncide par exemple avec l'ensemble des matrices de la forme  $\begin{pmatrix} \lambda & L \\ 0 & M \end{pmatrix}$  avec  $\lambda = \frac{1}{\det(M)}$ ,  $(M, L)$  décrivant  $\text{GL}_{n-1}(\mathbb{F}_q) \times \mathbb{F}_q^{n-1}$ . Son image dans  $\text{PSL}_n(\mathbb{F}_q)$  est un sous-groupe d'indice  $\frac{q^n - 1}{q - 1}$  de  $\text{PSL}_n(\mathbb{F}_q)$ .

## 1 PRÉLIMINAIRES

Cette partie collecte deux types de préliminaires — une rapide introduction au concept de *2-transitivité*, puis quelques résultats classiques sur les *matrices de Vandermonde* et l'*interpolation de Lagrange*.

### 1.1 ACTIONS 2-TRANSITIVES

Un rappel sur la *transitivité* s'impose peut-être pour commencer. Si  $G$  est un groupe et  $X$  un ensemble de cardinal  $n \geq 1$  sur lequel  $G$  opère, on dit que l'action de  $G$  sur  $X$  est *transitive* ou que  $G$  est *transitif sur  $X$*  si pour tous  $x, x' \in X$ , il existe un élément  $g$  de  $G$  pour lequel  $x' = g \cdot x$ . Dans ce cas :  $|G : G_x| = n$  pour tout  $x \in X$  si on note  $G_x$  le stabilisateur de  $x$  dans  $G$ . En particulier,  $|G|$  est divisible par  $n$ .

**Définition-théorème 3 (Action 2-transitive)** Soient  $G$  un groupe et  $X$  un ensemble de cardinal  $n \geq 2$  sur lequel  $G$  opère. On dit que l'action de  $G$  sur  $X$  est *2-transitive* ou que  $G$  est *2-transitif sur  $X$*  si l'action composante par composante de  $G$  sur l'ensemble des couples d'éléments distincts de  $X$  est transitive, i.e. si pour tous  $(x, y), (x', y') \in X \times X$  avec  $x \neq y$  et  $x' \neq y'$ , il existe un élément  $g$  de  $G$  pour lequel  $x' = g \cdot x$  et  $y' = g \cdot y$ .

- (i) Si  $G$  est 2-transitif sur  $X$ ,  $G$  est transitif sur  $X$ .
- (ii) Si  $G$  est 2-transitif sur  $X$ , le stabilisateur  $G_x$  de  $x$  dans  $G$  est transitif sur  $X \setminus \{x\}$  pour tout  $x \in X$ .

Nous n'en aurons pas besoin, mais la réciproque est vraie si  $n \geq 3$ .

- (iii) Si  $G$  est 2-transitif sur  $X$ ,  $|G|$  est divisible par  $n(n - 1)$ . En particulier,  $|G|$  est d'ordre pair.

#### Démonstration

- (i) Soient  $x, x' \in X$ . Si  $x = x'$  :  $x' = 1 \cdot x$ . Dans le cas contraire, il existe un élément  $g$  de  $G$  pour lequel  $x' = g \cdot x$  et  $x = g \cdot x'$ . Dans les deux cas :  $x' = g \cdot x$  pour un certain  $g \in G$ .
- (ii) Supposons  $G$  2-transitif sur  $X$  et fixons  $x \in X$ . Pour tous  $y, y' \in X \setminus \{x\}$ , il existe un élément  $g$  de  $G$  pour lequel  $x = g \cdot x$  et  $y' = g \cdot y$ , autrement dit un élément  $g$  de  $G_x$  pour lequel  $y' = g \cdot y$ . Comme voulu,  $G_x$  est transitif sur  $X \setminus \{x\}$ .

Pour la réciproque, faisons l'hypothèse que  $n \geq 3$  et que  $G_x$  est transitif sur  $X \setminus \{x\}$  pour tout  $x \in X$ . Soient  $(x, y), (x', y') \in X \times X$  avec  $x \neq y$  et  $x' \neq y'$ .

- Si  $x \neq y'$ , il existe un élément  $g_1$  de  $G_x$  pour lequel  $y' = g_1 \cdot y$ , puis un élément  $g_2$  de  $G_{y'}$  pour lequel  $x' = g_2 \cdot x$ . Si on pose  $g = g_2 g_1$ , alors comme voulu :  $g \cdot x = g_2 \cdot (g_1 \cdot x) = g_2 \cdot x = x'$  et  $g \cdot y = g_2 \cdot (g_1 \cdot y) = g_2 \cdot y' = y'$ . On raisonne de la même manière dans le cas où  $y \neq x'$ .
- Si  $x = y'$  et  $y = x'$ , nous cherchons un élément  $g$  de  $G$  pour lequel  $y = g \cdot x$  et  $x = g \cdot y$ . Un tel élément  $g$  est impossible à trouver si  $n = 2$  et si l'action de  $G$  sur  $X$  est triviale, mais comme  $n \geq 3$ , nous pouvons nous donner un élément  $z$  de  $X$  distinct de  $x$  et  $y$ . Aussitôt, par transitivité de  $G_z$  sur  $X \setminus \{z\}$ , il existe un élément  $g$  de  $G$  pour lequel  $y = g \cdot x$  et  $x = g \cdot y$ .

- (iii) Soient  $x, y \in X$  avec  $x \neq y$ . D'après (i),  $G$  est transitif sur  $X$ , donc  $|G : G_x| = n$ . De même,  $G_x$  est transitif sur  $X \setminus \{x\}$  d'après (ii), donc en notant  $G_{x,y}$  le stabilisateur de  $y$  dans  $G_x$  :  $|G_x : G_{x,y}| = n - 1$ . A fortiori :  $|G : G_{x,y}| = |G : G_x| \cdot |G_x : G_{x,y}| = n(n - 1)$ . ■

À présent, pour tout  $n \geq 1$  (resp.  $n \geq 2$ ), on dit qu'un sous-groupe du groupe symétrique  $S_n$  est *transitif* (resp. *2-transitif*) si son action naturelle sur  $\llbracket 1, n \rrbracket$  est transitive (resp. 2-transitive) au sens précédent. Il nous est maintenant possible de déduire le théorème 1 du théorème de Burnside 2.

**Démonstration (du théorème 1)** Soit  $G$  un groupe fini simple non abélien qui possède un sous-groupe  $H$  d'indice premier  $p$ .

- L'action de  $G$  sur l'ensemble  $G/H$  des classes à droite de  $G$  modulo  $H$  est transitive et définit un morphisme de groupes  $\varphi$  de  $G$  dans le groupe symétrique  $S_{G/H}$  dont le noyau est l'intersection des conjugués de  $H$  dans  $G$ . Or ce noyau est ici forcément trivial, car il est distingué dans  $G$  et inclus dans  $H$  alors que  $G$  est simple. Le morphisme  $\varphi$  plonge ainsi  $G$  dans  $S_{G/H}$  et l'identifie à un sous-groupe transitif de  $S_p$  car  $|G : H| = p$ .
- D'après le théorème de Burnside 2 momentanément admis,  $G$  est aussitôt soit 2-transitif, soit résoluble. Or s'il est résoluble, sa simplicité en fait un groupe cyclique d'ordre premier, donc abélien — ce qui est faux par hypothèse. Conclusion :  $G$  est 2-transitif et son ordre est divisible par  $p(p-1)$  d'après 3, donc par 2. ■

Comme la preuve qui s'achève le montre, un groupe fini simple non abélien qui possède un sous-groupe d'indice premier  $p$  n'est pas seulement d'ordre pair, il est en réalité d'ordre divisible par  $p(p-1)$ .

## 1.2 MATRICES DE VANDERMONDE ET INTERPOLATION DE LAGRANGE

**Définition-théorème 4 (Inversibilité des matrices de Vandermonde)** Soient  $K$  un corps et  $x_1, \dots, x_n \in K$ .

La matrice : 
$$V(x_1, \dots, x_n) = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix},$$
 appelée *matrice de Vandermonde* de  $x_1, \dots, x_n$ , est inversible si et seulement si les scalaires  $x_1, \dots, x_n$  sont distincts.

**Démonstration** Si deux des scalaires  $x_1, \dots, x_n$  sont égaux, la matrice  $V(x_1, \dots, x_n)$  a deux lignes égales donc n'est pas inversible. Pour la réciproque, supposons  $x_1, \dots, x_n$  distincts et montrons que le noyau de la matrice  $V(x_1, \dots, x_n)$  est trivial. Or pour tout  $(a_0, \dots, a_{n-1}) \in \text{Ker } V(x_1, \dots, x_n)$  :  $a_0 + a_1x_i + a_2x_i^2 + \dots + a_{n-1}x_i^{n-1} = 0$  pour tout  $i \in \llbracket 1, n \rrbracket$ , donc le polynôme  $a_0 + a_1X + \dots + a_{n-1}X^{n-1}$  admet  $x_1, \dots, x_n$  pour racines. De degré inférieur ou égal à  $n-1$ , ce polynôme est aussitôt nul, donc en effet  $a_0 = \dots = a_{n-1} = 0$ . ■

**Corollaire 5 (Sommes de puissances)** Soient  $K$  un corps et  $x_1, \dots, x_n \in K$  non tous nuls et distincts.

L'une des sommes  $\sum_{k=1}^n x_k, \sum_{k=1}^n x_k^2, \dots, \sum_{k=1}^n x_k^n$  au moins est non nulle.

**Démonstration** Tout simplement :  $(x_1 \cdots x_n) \times V(x_1, \dots, x_n) = \left( \sum_{k=1}^n x_k \quad \sum_{k=1}^n x_k^2 \quad \cdots \quad \sum_{k=1}^n x_k^n \right)$ .

Or la matrice  $V(x_1, \dots, x_n)$  est inversible d'après 4 et la matrice ligne  $(x_1 \cdots x_n)$  est non nulle, donc la matrice ligne  $\left( \sum_{k=1}^n x_k \quad \sum_{k=1}^n x_k^2 \quad \cdots \quad \sum_{k=1}^n x_k^n \right)$  est non nulle elle aussi. ■

**Théorème 6 (Interpolation de Lagrange de degré minimal)** Soient  $K$  un corps et  $x_1, \dots, x_n \in K$  distincts. Pour toute famille  $(y_1, \dots, y_n) \in K^n$ , il existe un et un seul polynôme  $P \in K[X]$  de degré inférieur ou égal à  $n-1$  pour lequel pour tout  $i \in \llbracket 1, n \rrbracket$  :  $P(x_i) = y_i$ .

**Démonstration** Soient  $(y_1, \dots, y_n) \in K^n$  et  $P = \sum_{k=0}^{n-1} a_k X^k \in K[X]$  de degré inférieur ou égal à  $n-1$ . Aussitôt : 
$$\forall i \in \llbracket 1, n \rrbracket, P(x_i) = y_i \iff \forall i \in \llbracket 1, n \rrbracket, \sum_{k=0}^{n-1} a_k x_i^k = y_i \iff V(x_1, \dots, x_n) \times \begin{pmatrix} a_0 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} y_0 \\ \vdots \\ y_{n-1} \end{pmatrix}.$$

L'existence et l'unicité de  $P$  découlent ainsi clairement de l'inversibilité de  $V(x_1, \dots, x_n)$  — théorème 4. ■

**Corollaire 7 (Fonctions définies sur un corps fini)** Soit  $p$  un nombre premier. Pour toute fonction  $f : \mathbb{F}_p \rightarrow \mathbb{F}_p$ , il existe un et un seul polynôme  $P \in \mathbb{F}_p[X]$  de degré inférieur ou égal à  $p-1$  pour lequel pour tout  $x \in \mathbb{F}_p$  :  $f(x) = P(x)$ .

En particulier, toute fonction de  $\mathbb{F}_p$  dans lui-même est polynomiale. Quelle différence avec les corps  $\mathbb{R}$  et  $\mathbb{C}$  !

**Démonstration** Il suffit d'appliquer le théorème 6 au corps  $K = \mathbb{F}_p$  avec pour tout  $i \in \llbracket 0, p-1 \rrbracket$  :  $x_i = i \in \mathbb{F}_p$  et  $y_i = f(x_i)$ . ■

Les corollaires 5 et 7 joueront un rôle crucial dans la suite de ce texte.

## 2 UN THÉORÈME DE SCHUR AU SERVICE DE BURNSIDE

Le théorème qui suit date de 1908 et nous n'étudierons pas tout à fait la preuve qu'en a proposée Schur, car un certain Peter Müller l'a simplifiée avec élégance en 2008. En tout cas, c'est pour redémontrer le théorème de Burnside que Schur a développé les idées qui suivent.

**Théorème 8 (Un théorème de Schur)** Soient  $p$  un nombre premier et  $\sigma$  une permutation de  $\mathbb{F}_p$ . On suppose qu'il existe une partie  $U$  de  $\mathbb{F}_p^*$  à la fois non vide et distincte de  $\mathbb{F}_p^*$  pour laquelle pour tous  $x, y \in \mathbb{F}_p$  :

$$x - y \in U \implies \sigma(x) - \sigma(y) \in U.$$

La permutation  $\sigma$  est alors affine, i.e. de la forme  $x \mapsto ax + b$  pour certains  $a \in \mathbb{F}_p^*$  et  $b \in \mathbb{F}_p$ .

Avant d'établir ce théorème, nous commencerons par en déduire le théorème de Burnside 2 qui est notre objectif véritable.

**Démonstration (du théorème 2)** Soient  $p$  un nombre premier et  $G$  un sous-groupe transitif, mais non 2-transitif, de  $S_p$ .

- Pour commencer,  $G$  est d'ordre divisible par  $p$  en tant que sous-groupe transitif de  $S_p$ , donc contient une permutation d'ordre  $p$ , qui dans  $S_p$  ne peut être qu'un  $p$ -cycle  $(x_0 \dots x_{p-1})$ . Ce  $p$ -cycle nous permet de voir  $G$  comme un groupe de permutations de  $\mathbb{F}_p$  si l'on identifie pour tout  $k \in \llbracket 0, p-1 \rrbracket$  l'élément  $x_k$  de  $\llbracket 1, p \rrbracket$  à l'image de  $k$  dans  $\mathbb{F}_p$ . Le  $p$ -cycle  $(x_0 \dots x_{p-1})$  est dans ces conditions identifié à la translation  $x \mapsto x + 1$  de  $\mathbb{F}_p$  que nous noterons  $\theta$ . Avec ce nouveau point de vue, le stabilisateur  $G_0$  de 0 dans  $G$  permute  $\mathbb{F}_p^*$ , et il le fait de plus en découpant au moins deux orbites d'après 3 car  $G$  n'est pas 2-transitif. Notons  $U$  l'une quelconque de ces orbites — une partie de  $\mathbb{F}_p^*$  à la fois non vide et distincte de  $\mathbb{F}_p^*$ .

- À présent, soit  $\sigma \in G$  et  $x, y \in U$ . Aussitôt :

$$\theta^{-\sigma(y)}\sigma\theta^y(0) = \theta^{-\sigma(y)}\sigma(y) = \sigma(y) - \sigma(y) = 0, \quad \text{donc } \theta^{-\sigma(y)}\sigma\theta^y \in G_0,$$

et par ailleurs :  $\theta^{-\sigma(y)}\sigma\theta^y(x - y) = \theta^{-\sigma(y)}\sigma(x) = \sigma(x) - \sigma(y)$ . Sous l'hypothèse que  $x - y \in U$ , on peut ainsi affirmer que  $\theta^{-\sigma(y)}\sigma\theta^y(x - y) \in U$ , i.e. que  $\sigma(x) - \sigma(y) \in U$ . Il en découle que  $\sigma$  est affine d'après le théorème de Schur 8. Ainsi,  $G$  est inclus tout entier dans le groupe affine  $\text{GA}(\mathbb{F}_p)$  de  $\mathbb{F}_p$ . ■

**Démonstration (du théorème de Schur 8)** D'après 7, il existe un unique polynôme  $P \in \mathbb{F}_p[X]$  de degré  $d$  inférieur ou égal à  $p-1$  pour lequel pour tout  $x \in \mathbb{F}_p$  :  $P(x) = \sigma(x)$ . Clairement,  $P$  n'est pas constant, donc  $d \geq 1$ , et pour montrer que  $\sigma$  est affine, il nous suffit de prouver que  $d = 1$ .

- Montrons d'abord que l'ensemble  $U$  peut être choisi de cardinal inférieur ou égal à  $\frac{p-1}{2}$ .  
Pour tous  $x, y \in \mathbb{F}_p$ , si  $\sigma(x) - \sigma(y) \in U$ , alors par définition de  $U$  :  $\sigma^k(x) - \sigma^k(y) \in U$  pour tout  $k \in \mathbb{N}^*$ , donc en particulier  $x - y = \sigma^{|\sigma|}(x) - \sigma^{|\sigma|}(y) \in U$ . Par contraposition, nous venons de montrer que pour tous  $x, y \in \mathbb{F}_p$  :  $x - y \in \mathbb{F}_p^* \setminus U \implies \sigma(x) - \sigma(y) \in \mathbb{F}_p^* \setminus U$ , autrement dit que l'ensemble  $\mathbb{F}_p^* \setminus U$  a la même propriété que l'ensemble  $U$ . Comme l'un de ces deux ensembles est de cardinal inférieur ou égal à  $\frac{p-1}{2}$ , nous pouvons imposer à  $U$  l'inégalité  $|U| \leq \frac{p-1}{2}$  quitte à le remplacer par son complémentaire.

- À présent, soit  $x \in \mathbb{F}_p$  fixé. Pour tout  $u \in U$  :  $(x+u) - x \in U$ , donc  $\sigma(x+u) - \sigma(x) \in U$  par définition de  $U$ . L'application  $u \mapsto \sigma(x+u) - \sigma(x)$  se trouve ainsi définie de  $U$  dans  $U$ , et c'est même une bijection de  $U$  sur  $U$  car  $\sigma$  est une permutation. Conclusion :  $\{\sigma(x+u) \mid u \in U\} = \{\sigma(x) + u \mid u \in U\}$ , donc a fortiori  $\sum_{u \in U} \sigma(x+u)^n = \sum_{u \in U} (\sigma(x) + u)^n$  pour tout  $n \in \mathbb{N}^*$ , et ceci pour tout  $x \in \mathbb{F}_p$ .

Si on impose à  $n$  l'inégalité  $dn \leq p-1$ , le polynôme  $\sum_{u \in U} (P(X+u)^n - (P(X)+u)^n)$  est nul car il possède trop de racines, donc  $\sum_{u \in U} P(X+u)^n = \sum_{u \in U} (P(X)+u)^n$ .

- Pour faire parler cette identité, posons  $s_i = \sum_{u \in U} u^i$  pour tout  $i \in \mathbb{N}^*$ . Grâce au théorème 5, nous pouvons noter  $m$  le plus petit entier  $i \in \mathbb{N}^*$  pour lequel  $s_i \neq 0$ , avec en l'occurrence  $m \leq |U| \leq \frac{p-1}{2}$ . Aussitôt :

$$\sum_{u \in U} (P(X+u)^n - P(X)^n) = \sum_{u \in U} ((P(X)+u)^n - P(X)^n) = \sum_{u \in U} \sum_{k=1}^n \binom{n}{k} u^k P(X)^{n-k} = \sum_{k=1}^n \binom{n}{k} s_k P(X)^{n-k} = \sum_{k=m}^n \binom{n}{k} s_k P(X)^{n-k}.$$

Dans cette identité, le polynôme de droite est de degré inférieur ou égal à  $d(n-m)$ , mais l'analyse du degré du polynôme de gauche n'est pas aussi aisée — aussi allons-nous ruser et « lisser » cette identité. Le résultat découlera du double calcul de degré auquel nous aurons ainsi procédé.

- De quelle manière? La famille  $(P(X)^n, (P(X)^n)', (P(X)^n)'', \dots, (P(X)^n)^{(dn)})$  est échelonnée en degré et constituée de  $dn+1$  polynômes non nuls de degré inférieur ou égal à  $dn$ , c'est donc une base de  $(\mathbb{F}_p)_{dn}[X]$ .

En particulier, pour certains  $\lambda_0, \dots, \lambda_{dn} \in \mathbb{F}_p$  :  $X^{dn} = \sum_{i=0}^{dn} \lambda_i (P(X)^n)^{(i)}$ , avec par ailleurs  $\lambda_0 \neq 0$ . Ainsi :

$$\begin{aligned} \sum_{u \in U} ((X+u)^{dn} - X^{dn}) &= \sum_{u \in U} \left( \sum_{i=0}^{dn} \lambda_i (P(X+u)^n)^{(i)} - \sum_{i=0}^{dn} \lambda_i (P(X)^n)^{(i)} \right) \\ &= \sum_{i=0}^{dn} \lambda_i \left( \sum_{u \in U} (P(X+u)^n - P(X)^n) \right)^{(i)} = \sum_{i=0}^{dn} \lambda_i \left( \sum_{k=m}^n \binom{n}{k} s_k P(X)^{n-k} \right)^{(i)}. \end{aligned}$$

À droite, le degré n'a pas changé car  $\lambda_0 \neq 0$ , le polynôme est toujours de degré inférieur ou égal à  $d(n-m)$ . À gauche, en revanche, la situation est maintenant plus lisible :

$$\sum_{u \in U} ((X+u)^{dn} - X^{dn}) = \sum_{u \in U} \sum_{k=1}^{dn} \binom{dn}{k} u^k X^{dn-k} = \sum_{k=1}^{dn} \binom{dn}{k} s_k X^{dn-k}.$$

Si  $m > dn$ , le polynôme obtenu est nul, ce dont nous ne pouvons rien tirer. Pour le moment, cela dit, nous avons juste imposé à  $n$  l'inégalité  $dn \leq p-1$ . Imposons-lui en outre d'être maximal pour cette inégalité.

Dans ces conditions  $d(n+1) > p-1$ , donc  $2dn > p-1$ , puis aussitôt  $m \leq \frac{p-1}{2} < dn$ . Dans l'égalité polynomiale qui précède, le polynôme  $\sum_{u \in U} ((X+u)^{dn} - X^{dn})$  est maintenant clairement de degré  $dn-m$ , car comme  $dn \leq p-1$ , les coefficients binomiaux  $\binom{dn}{k}$  sont non nuls dans  $\mathbb{F}_p$ . Par un double calcul de degré, nous venons d'établir l'inégalité  $dn-m \leq d(n-m)$ , et enfin  $d=1$ . ■