Rappels : Pour tout naturel q, il existe un corps fini ayant q éléments *si et seulement si* q s'écrit de la forme p^d avec p un nombre premier et $d \geq 1$; dans ce cas, le corps en question est unique à isomorphisme près et on le note $\mathbb{F}_q$: il est de caractéristique p et a $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ comme corps premier, sur lequel il est de degré d. Le corps $\mathbb{F}_q$, avec $q = p^d$, peut être vu comme un sous-corps de $\mathbb{F}_{q'}$, avec $q' = p'^{d'}$, si et seulement si $p' = p$ et $d|d'$, auquel cas ce sous-corps est unique (et $\mathbb{F}_q$ se voit comme l'ensemble des racines du polynôme $t^q - t$ dans $\mathbb{F}_{q'}$; inversement, $\mathbb{F}_{q'}$ se voit comme un corps de décomposition de $t^{q'} - t$ dans $\mathbb{F}_q$). Le groupe multiplicatif $\mathbb{F}_q^\times$ de $\mathbb{F}_q$ — comme tout groupe multiplicatif fini d'un corps — est cyclique, c'est le groupe des racines $(q-1)$-ièmes de l'unité dans $\mathbb{F}_q$. Le groupe des automorphismes de $\mathbb{F}_{q'}$ laissant fixe $\mathbb{F}_q$, ou groupe de Galois de $\mathbb{F}_{q'}$ sur $\mathbb{F}_q$, est cyclique d'ordre d'/d engendré par le frobenius à la puissance d, soit $\mathrm{Fr}^d : x \mapsto x^q$.

1. Soit $q = p^d$ (où p est un nombre premier et $d \geq 1$) et soit $k \geq 1$ un entier naturel. Le nombre de polynômes unitaires de degré k dans $\mathbb{F}_q$ est manifestement q^k. Montrer que le nombre de polynômes unitaires de degré k sur $\mathbb{F}_q$ qui sont irréductibles est

$$\frac{1}{k} \sum_{\ell | k} \mu(\ell)\, q^{k/\ell}$$

où ℓ parcourt les diviseurs de k et $\mu(\ell)$ désigne la fonction de Möbius[1]. (Indication : compter les éléments de $\mathbb{F}_{q^k}$ en fonction de leur degré sur $\mathbb{F}_q$, ou bien regarder les orbites par l'action du groupe de Galois $G = \langle \mathrm{Fr}^d \rangle$ sur $\mathbb{F}_{q^k}$.) On dit qu'un tel polynôme est *primitif* lorsque, de plus, une de ses racines (et donc n'importe laquelle de ses racines) est un générateur du groupe multiplicatif $\mathbb{F}_{q^k}^\times$: montrer que le nombre de polynômes unitaires irréductibles de degré k sur $\mathbb{F}_q$ qui sont primitifs est

$$\frac{1}{k}\, \phi(q^k - 1)$$

où $\phi(n)$ désigne la fonction indicatrice d'Euler[2]. Calculer ces valeurs pour $q = 2$ et $k = 6$.

Corrigé. Commençons par une observation : si $P \in \mathbb{F}_q[t]$ est un polynôme irréductible à coefficients dans $\mathbb{F}_q$, disons unitaire de degré k, alors il est complètement décomposé sur son corps de rupture $\mathbb{F}_{q^k}$ (i.e. : dès qu'il acquiert une racine, il les acquiert toutes) ; ceci découle immédiatement de l'unicité de $\mathbb{F}_{q^k}$ dans n'importe quel corps le contenant (autrement dit, n'importe quel élément algébrique de degré k sur $\mathbb{F}_q$, et en particulier toute racine de P, engendre le même corps $\mathbb{F}_{q^k}$).

Si P est un polynôme irréductible de degré k sur $\mathbb{F}_q$, ses racines dans $\mathbb{F}_{q^k}$ sont au nombre de k exactement (elles sont un ensemble de conjugués, c'est-à-dire une orbite pour l'action du groupe de Galois $G = \langle \mathrm{Fr}^d \rangle$ sur $\mathbb{F}_{q^k}$). De plus, tout élément de $\mathbb{F}_{q^k}$ qui est de degré précisément k sur $\mathbb{F}_q$, c'est-à-dire n'est pas dans un $\mathbb{F}_{q^{k_1}}$ pour $k_1 < k$ (diviseur strict), est racine d'un unique polynôme unitaire irréductible de degré k sur $\mathbb{F}_q$. Ainsi, si $M(\ell)$ désigne le nombre d'éléments de $\mathbb{F}_{q^k}$ (ou de $\mathbb{F}_{q^\ell}$) de degré ℓ sur $\mathbb{F}_q$, le nombre de polynômes unitaires irréductibles de degré k sur $\mathbb{F}_q$ est $\frac{1}{k} M(k)$, et on a $q^k = \sum_{\ell | k} M(\ell)$ (pour tout entier naturel non nul k).

On voit alors que le nombre $M(k)$ d'éléments de degré exactement k sur $\mathbb{F}_q$ est égal à q^k moins les $M(k/\ell)$ pour ℓ diviseur premier de k : c'est-à-dire q^k moins $q^{k/\ell}$ pour tout ℓ diviseur premier de k plus $q^{k/\ell\ell'}$ pour ℓ, ℓ' diviseurs premiers distincts de k (car on a décompté deux fois ces éléments) plus, etc., ce qui est la formule annoncée. Plus rigoureusement, comme $q^k = \sum_{\ell | k} M(\ell)$, en appliquant la formule d'inversion de Möbius, on a $M(k) = \sum_{\ell | k} \mu(\ell)\, q^{k/\ell}$, d'où le résultat.

Enfin, le nombre de générateurs du groupe $\mathbb{F}_{q^k}^\times$ à $q^k - 1$ éléments est $\phi(q^k - 1)$. N'importe lequel de ces générateurs est de degré exactement k sur $\mathbb{F}_q$ (car s'il est dans un $\mathbb{F}_{q^{k_1}}$ pour $k_1 < k$

([1]) Soit $\mu(n) = 0$ si n est divisible par un carré et $\mu(n) = (-1)^s$ sinon, avec s le nombre de facteurs premiers — évidemment distincts — de n.
([2]) Soit $\phi(n) = \mathrm{card}((\mathbb{Z}/n\mathbb{Z})^\times)$.

il est d'ordre multiplicatif au mieux $q^{k_1}-1$). Le nombre de polynômes unitaires irréductibles primitifs de degré k est donc bien $\frac{1}{k}\,\phi(q^k-1)$.

Pour $q=2$ et $k=6$, il y a $2^6=64$ polynômes unitaires de degré k sur $\mathbb{F}_q$, le nombre de ceux qui sont irréductibles est $\frac{1}{6}\,(2^6-2^3-2^2+2^1)=\frac{1}{6}\,54=9$, et le nombre de ceux-là qui sont primitifs est $\frac{1}{6}\,\phi(3^2\cdot 7)=\frac{1}{6}\,(2\times 3\times 6)=6$. ✓

2 (théorème de Chevalley-Warning). Soit $\mathbb{F}=\mathbb{F}_q$ un corps fini (de caractéristique p), et $P\in\mathbb{F}[X_0,\dots,X_n]$ un polynôme homogène de degré $d>0$ en $n+1$ variables avec $d\leq n$: on cherche à montrer que P a un zéro non trivial (c'est-à-dire autre que $(0,\dots,0)$). (En termes géométriques : une hypersurface de degré $d\leq n$ dans $\mathbb{P}^n$ sur un corps fini $\mathbb{F}$ a toujours un point sur $\mathbb{F}$.) Pour cela, on montrera que le nombre de zéros de P dans $\mathbb{F}^{n+1}$ est multiple de p, en considérant la somme des $P(x_0,\dots,x_n)^{q-1}$ où $(x_0,\dots,x_n)$ parcourt tous les $(n+1)$-uplets d'éléments de $\mathbb{F}$.

Corrigé. Remarquons que pour $t\in\mathbb{F}$ on a $t^{q-1}=1$ sauf si $t=0$ auquel cas $t^{q-1}=0$. Ainsi, la somme des $P(x_0,\dots,x_n)^{q-1}$ est congrue modulo p au nombre de $(x_0,\dots,x_n)$ tels que $P(x_0,\dots,x_n)\neq 0$, donc si on prouve qu'elle est nulle (dans $\mathbb{F}$) le nombre de zéros de P dans $\mathbb{F}^{n+1}$ sera multiple de p (le cardinal de tout $\mathbb{F}^{n+1}$ étant lui-même multiple de p), et, comme il existe toujours le zéro trivial, il y en aura au moins un autre.

En développant $P(x_0,\dots,x_n)^{q-1}$ comme somme de monômes chacun de degré $d(q-1)$, on est ramené à prouver que si $x_0^{s_0}\cdots x_n^{s_n}$ est un monôme de degré $s_0+\cdots+s_n=d(q-1)<(n+1)(q-1)$ alors la somme sur tous les $(x_0,\dots,x_n)$ de $x_0^{s_0}\cdots x_n^{s_n}$ est nulle dans $\mathbb{F}$. Cette somme se factorise comme le produit des $\sum_{x\in\mathbb{F}}x^{s_i}$ et il suffit donc de prouver qu'au moins l'un de ces facteurs est nul. Or au moins un des s_i vérifie $s_i<q-1$. Finalement, il suffit donc prouver que si $s<q-1$ alors $\sum_{x\in\mathbb{F}}x^s=0$ (dans $\mathbb{F}$).

Lorsque $s=0$, le résultat est clair (le nombre d'éléments de $\mathbb{F}$ est multiple de p), on peut donc supposer $s>0$ et la somme peut être faite sur $\mathbb{F}^\times$, qui est un groupe cyclique d'ordre $q-1$: en appelant g un générateur de celui-ci, on a $\sum_{x\in\mathbb{F}^\times}x^s=\sum_{i=0}^{q-2}g^{si}=\frac{g^{s(q-1)}-1}{g^s-1}$ (puisque $g^s\neq 1$ dans $\mathbb{F}$) et comme $g^{s(q-1)}=1$, cette somme est bien nulle, ce qui conclut. ✓

3 (« petit » théorème de Wedderburn). Soit D une algèbre à divisions (= corps gauche) finie (de cardinal fini). On se propose de montrer que D est, en fait, un corps. Soit $\mathbb{F}$ le centre de D (c'est-à-dire l'ensemble des $x\in D$ tels que $(\forall y\in D)(xy=yx)$), qui est un corps fini, et q son cardinal, et soit n la dimension de D comme $\mathbb{F}$-espace vectoriel. Écrire l'équation aux classes pour l'action de $D^\times$ sur lui-même par conjugaison. En notant $\Phi_n\in\mathbb{Z}[t]$ le n-ième polynôme cyclotomique, en déduire que $\Phi_n(q)$ divise $q-1$. Obtenir une contradiction si $n>1$ en prouvant que $|\Phi_n(q)|>q-1$.

Corrigé. Pour tout $x\in D$, soit $Z_x=\{y\in D : xy=yx\}$ le centralisateur de x : manifestement, Z_x est un $\mathbb{F}$-espace vectoriel, et même une algèbre à divisions sur $\mathbb{F}$. Soit $d(x)$ sa dimension (comme $\mathbb{F}$-espace vectoriel) : alors $Z_x\cap D^\times$ a pour cardinal $q^{d(x)}-1$, où $d(x)$ divise n (par exemple parce que D est un Z_x-espace vectoriel à gauche, ou simplement parce que $q^{d(x)}-1$ ne peut diviser q^n-1 que si $d(x)$ divise n). L'orbite de x sous l'action de $D^\times$ a pour cardinal $\frac{q^n-1}{q^{d(x)}-1}$, et l'équation aux classes (le cardinal de $D^\times$ est la somme des cardinaux des orbites) s'écrit

$$q^n-1\;=\;q-1\;+\;\sum_{x\in S}\frac{q^n-1}{q^{d(x)}-1}$$

(où S est un ensemble de représentants des orbites ayant strictement plus d'un seul élément et $q-1$ est le cardinal de $\mathbb{F}^\times$, ensemble des orbites à un élément).

Soit $\Phi_n(t) = \prod(t-\zeta)$ (le produit portant sur les racines primitives n-ièmes de l'unité) le n-ième polynôme cyclotomique : rappelons que $\Phi_n \in \mathbb{Z}[t]$. Alors $\Phi_n(q)$ divise q^n-1, et même divise $\frac{q^n-1}{q^{d(x)}-1} = \prod_{d(x)|\ell|n,\ \ell>d(x)} \Phi_\ell(q)$ pour $d(x) < n$ (soit x non central). On en déduit que $\Phi_n(q)$ divise $q-1$ et en particulier $|\Phi_n(q)| \leq |q-1|$. Mais comme $|q-\zeta| > |q-1|$ pour tout complexe $\zeta \neq 1$ sur le cercle unité, ce n'est possible que si $n=1$, et $D = \mathbb{F}$, ce qu'on voulait prouver. ✓

4 (loi de réciprocité quadratique). Si p est un nombre premier impair, et n un entier non multiple de p (ou un élément de $\mathbb{F}_p^\times$), on définit le symbole de Legendre $\left(\frac{n}{p}\right)$ comme $+1$ si n est un carré dans $\mathbb{F}_p$, et -1 sinon. Remarquer que $\left(\frac{mn}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{n}{p}\right)$ et que $\left(\frac{n}{p}\right) \equiv n^{(p-1)/2} \pmod p$. Soient maintenant p et q deux nombres premiers impairs distincts, et soit ζ une racine primitive p-ième de l'unité dans une extension de $\mathbb{F}_q$. Posons $S = \sum_{x\in\mathbb{F}_p^\times}\left(\frac{x}{p}\right)\zeta^x \in \mathbb{F}_q$: montrer que $S^2 = \left(\frac{-1}{p}\right)p$ et que $S^q = \left(\frac{q}{p}\right)S$. En déduire la *loi de réciprocité quadratique* :

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}$$

Corrigé. Expliquons d'abord pourquoi $\left(\frac{n}{p}\right) \equiv n^{(p-1)/2} \pmod p$: si g est un élément primitif modulo p, c'est-à-dire un générateur de $\mathbb{F}_p^\times$, alors un élément n de $\mathbb{F}_p^\times$ est un carré si et seulement si il s'écrit $n = g^{2i}$ pour un certain i, et alors $n^{(p-1)/2} = g^{i(p-1)} = 1$ dans $\mathbb{F}_p^\times$ tandis que si à l'inverse $n = g^{2i+1}$ alors $n^{(p-1)/2} = g^{i(p-1)}\, g^{(p-1)/2} = -1$ (car $g^{(p-1)/2}$ a pour carré 1 dans $\mathbb{F}_p$ et ne vaut pas lui-même 1). En particulier, on peut remarquer $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, dans $\mathbb{Z}$ cette fois. Le fait que $\left(\frac{mn}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{n}{p}\right)$ est également clair.

On a $S^2 = \sum_{x,y\in\mathbb{F}_p^\times}\left(\frac{xy}{p}\right)\zeta^{x+y}$, soit, en posant $t = y/x$ (dans $\mathbb{F}_p^\times$), $\sum_{x,t\in\mathbb{F}_p^\times}\left(\frac{t}{p}\right)\zeta^{x(1+t)}$ (où on a utilisé le fait que $\left(\frac{x}{p}\right)^2 = 1$). Or $\sum_{x\in\mathbb{F}_p^\times}\zeta^{xu}$ vaut (toujours dans $\mathbb{F}_q$) -1 si $u \in \mathbb{F}_p^\times$ et $p-1$ si $u = 0$: appliquant ce fait dans ce qui précède à $u = 1+t$, on trouve $S^2 = \left(\frac{-1}{p}\right)p - \sum_{x,t\in\mathbb{F}_p^\times}\left(\frac{t}{p}\right)$ et le second terme est nul (il y a autant d'éléments de $\mathbb{F}_p^\times$ qui sont des carrés que qui n'en sont pas) d'où $S^2 = \left(\frac{-1}{p}\right)p$.

Par ailleurs, $S^q = \sum_{x\in\mathbb{F}_p^\times}\left(\frac{x}{p}\right)\zeta^{qx}$ (le frobenius $x \mapsto x^q$ étant un automorphisme de corps) donc $S^q = \sum_{z\in\mathbb{F}_p^\times}\left(\frac{q}{p}\right)\left(\frac{z}{p}\right)\zeta^z$ (en posant $z = qx$ et en utilisant de nouveau le fait que $\left(\frac{q}{p}\right)$ est son inverse), soit $S^q = \left(\frac{q}{p}\right)S$.

De ces deux formules on déduit d'une part $S^{q-1} = \left(\frac{q}{p}\right)$ et de l'autre $S^{q-1} = (S^2)^{(q-1)/2} = \left[\left(\frac{-1}{p}\right)p\right]^{(q-1)/2} = (-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right)$, d'où la loi de réciprocité quadratique (l'égalité ayant lieu dans $\mathbb{F}_q$ donc dans $\mathbb{Z}$). ✓

5 (bracelets de De Bruijn). On appelle *bracelet de De Bruijn* d'ordre $k \geq 1$ sur un alphabet (ensemble) fini A à $q \geq 1$ éléments une application b de $\mathbb{Z}/q^k\mathbb{Z}$ vers A telle que pour tout k-uplet $(a_0, \ldots, a_{k-1})$ d'éléments de A il existe un $i \in \mathbb{Z}/q^k\mathbb{Z}$ (manifestement unique) pour lequel $a_0 = b(i)$, $a_1 = b(i+1)$ et ainsi de suite jusqu'à $a_{k-1} = b(i+k-1)$. Autrement dit, il s'agit d'un bracelet de longueur q^k sur les q perles de l'alphabet, qui contient toute combinaison

possible de k perles consécutives. On se propose de montrer que pour tout k et tout q il exite un bracelet de De Bruijn.

(1) Dans le cas où $q = p^d$ est une puissance d'un nombre premier p, montrer en utilisant le corps fini $\mathbb{F}_{q^k}$ qu'il existe un bracelet de De Bruijn. On pourra considérer g un générateur du groupe multiplicatif $\mathbb{F}_{q^k}^\times$ et décomposer les g^i dans la base $1, g, \dots, g^{k-1}$ de $\mathbb{F}_{q^k}$ sur $\mathbb{F}_q$. (Commencer par obtenir un « presque » bracelet de De Bruijn, de longueur $q^k - 1$, qui contient toutes combinaison de k perles sauf une.)

(2) Comment peut-on obtenir un bracelet de De Bruijn lorsque q n'est pas une puissance d'un nombre premier mais un produit de telles puissances (c'est-à-dire un entier naturel non nul quelconque) ?

Corrigé. (1) Manifestement, si g est un générateur du groupe multiplicatif $\mathbb{F}_{q^k}^\times$, les éléments $1, g, \dots, g^{k-1}$ sont libres sur $\mathbb{F}_q$, donc sont une $\mathbb{F}_q$-base de $\mathbb{F}_{q^k}$. Pour tout $i \in \mathbb{Z}$, posons $g^i = \alpha_0^{(i)} + \alpha_1^{(i)} g + \dots + \alpha_{k-1}^{(i)} g^{k-1}$. Montrons que la suite $(\alpha_0^{(i)})_i$ (périodique de période $p^k - 1$) est un « presque » bracelet de De Bruijn, en ce sens qu'il s'y trouve chaque k-uplet d'éléments de $\mathbb{F}_q$ à l'exception du k-uplet nul.

Remarquons d'abord que tout k-uplet à l'exception du k-uplet nul est la valeur pour un certain i de $(\alpha_0^{(i)}, \alpha_1^{(i)}, \dots, \alpha_{k-1}^{(i)})$ (puisqu'il existe bien un i pour lequel $g^i = \alpha_0^{(i)} + \alpha_1^{(i)} g + \dots + \alpha_{k-1}^{(i)} g^{k-1}$). Reste à expliquer pourquoi l'application $\mathbb{F}_q$-linéaire $\varphi\colon \mathbb{F}_{q^k} \to (\mathbb{F}_q)^k$ qui envoie $x \in \mathbb{F}_{q^k}$ sur les coordonnées respectives sur l'élément 1 (de la base $1, g, \dots, g^{k-1}$) de $gx, g^2x, \dots, g^kx$ (autrement dit, de façon peut-être plus claire, φ envoie $g^i = \alpha_0^{(i)} + \alpha_1^{(i)} g + \dots + \alpha_{k-1}^{(i)} g^{k-1}$ sur $(\alpha_0^{(i+1)}, \dots, \alpha_0^{(i+k)})$), est bijective. Or la matrice de φ sur la base $g^{k-1}, \dots, g, 1$ (au départ, et la base canonique à l'arrivée) est $(\alpha_0^{(k-j+i)})_{ji}$, donc triangulaire (car $\alpha_0^{(i)} = 0$ si $0 < i < k$) de diagonale $(\alpha_0^{(k)}, \dots, \alpha_0^{(k)})$, donc inversible ($\alpha_0^{(k)}$ ne peut pas être nul, sinon $\alpha_0^{(i)}$ serait nul pour tout $i > 0$ et on ne pourrait pas avoir $g^{p^k-1} = 1$).

Une fois obtenu un tel « presque » bracelet de De Bruijn, auquel il ne manque que le k-uplet $(0, \dots, 0)$, il suffit d'insérer une perle 0 supplémentaire dans une des séquences de $k - 1$ perles 0 (il y a $q - 1$ tels endroits). La longueur du bracelet passe alors de $p^k - 1$ à p^k, et on se convainc immédiatement que tout k-uplet qui se trouvait dans l'ancien bracelet se trouve aussi dans le nouveau, et que le k-uplet nul s'y trouve maintenant. On a donc obtenu le bracelet recherché.

(2) Soient $q_1, \dots, q_s$ des puissances de nombres premiers distincts, et soient $b_1, \dots, b_s$ des bracelets de De Bruijn d'ordre k sur des alphabets $A_1, \dots, A_s$ à $q_1, \dots, q_s$ éléments : cherchons à obtenir un bracelet de De Bruijn b d'ordre k sur un alphabet (quelconque) à $q = q_1 \cdots q_s$ lettres, mettons $A = A_1 \times \cdots \times A_s$. Pour cela, on définit simplement $b(i) = (b_1(i_1), \dots, b_s(i_s))$, où $i_1, \dots, i_s$ sont les réductions de $i \in \mathbb{Z}/q^k\mathbb{Z}$ respectivement modulo $q_1^k, \dots, q_s^k$. Le théorème chinois assure que pour tous éléments $i_1, \dots, i_s$ de $\mathbb{Z}/q_1^k\mathbb{Z}, \dots, \mathbb{Z}/q_s^k\mathbb{Z}$ respectivement, il existe un (unique) $i \in \mathbb{Z}/q^k\mathbb{Z}$ congru à $i_1, \dots, i_s$ modulo $q_1^k, \dots, q_s^k$ respectivement. Or ceci signifie précisément que pour tout k-uplet $(a_0, \dots, a_{k-1}) \in A^k$, une fois trouvés (comme $b_1, \dots, b_s$ sont des bracelets de De Bruijn) des indices $i_1, \dots, i_s$ dans les périodes respectives de $b_1, \dots, b_s$ où les k-uplets composantes de $(a_0, \dots, a_{k-1})$ dans $A_1^k, \dots, A_s^k$ se situent, on peut trouver un indice i modulo q^s où $(a_0, \dots, a_{k-1})$ se situe dans b. C'est-à-dire que b est bien un bracelet de De Bruijn. ✓

6 (addition et multiplication de Conway). Lorsque E est un ensemble d'entiers naturels (non égal à $\mathbb{N}$ tout entier), on notera $\operatorname{mex} E = \min(\mathbb{N} \setminus E)$ le plus petit naturel qui n'est pas dans E. On définit par récurrence des opérations binaires $\#$ et $@$ sur $\mathbb{N}$ (et à valeurs dans $\mathbb{N}$), appelées respectivement somme de Conway et produit de Conway (ou somme de nim et produit

de nim), en posant :

$$a\#b = \mathrm{mex}(\{a'\#b : a' < a\} \cup \{a\#b' : b' < b\})$$

$$a@b = \mathrm{mex}\{(a'@b)\#(a'@b')\#(a@b') : a' < a \text{ et } b' < b\}$$

(†) Montrer successivement, par des récurrences : que $\#$ est commutative, que $a\#0 = a$ pour tout naturel a, que $a\#b = 0$ si et seulement si $a = b$, que $\#$ est associative (supposer $e < a\#(b\#c)$ et prouver $e \neq (a\#b)\#c$ par exemple), que $@$ est commutative, que $a@0 = 0$ pour tout naturel a, que $a@1 = a$ pour tout naturel a, que $@$ est distributive sur $\#$, que $@$ est associative, et que $a@b = 0$ si et seulement si $a = 0$ ou $b = 0$. Expliquer comment l'écriture binaire de $a\#b$ (c'est-à-dire son unique décomposition en puissances de 2 distinctes) se calcule à partir de celles de a et de b. Calculer $2^{2^r}@2^{2^s}$ pour $r \neq s$ et $2^{2^r}@2^{2^r}$ et prouver que l'ensemble des entiers naturels entre 0 et $2^{2^r} - 1$ est stable par les lois $\#$ et $@$ et forme un corps (isomorphe, donc, à $\mathbb{F}_{2^{2^r}}$).

On considère le jeu suivant, appelé jeu de nim de dimension 2 : un damier rectangulaire de dimensions arbitraires est complètement rempli de pions, blancs d'un côté et noirs de l'autre (de sorte qu'une et une seule de ces couleurs est visible pour chaque pion), dans une certaine configuration initiale (non précisée). Chacun des deux joueurs, à son tour, doit retourner un pion de façon à le faire passer de noir à blanc, et il peut aussi retourner (quelle que soit sa couleur à ce moment-là) un pion quelconque plus haut dans la même colonne, ou un pion quelconque plus à gauche dans la même ligne, ou encore les deux à la fois à condition dans ce cas de retourner aussi le quatrième sommet du rectangle défini par les trois pions retournés. Le jeu se termine quand tous les pions sont blancs, de sorte que le joueur dont c'est le tour ne peut plus jouer, et ce joueur a alors perdu. Montrer que le jeu se termine toujours en temps fini, et que le second joueur a une stratégie gagnante si et seulement si la somme de Conway des $a@b$ est nulle, où (a, b) parcourt tous les couples ligne/colonne (comptées à partir de 1) où le pion est noir.

(‡) Montrer que, si on étend les lois $\#$ et $@$ à des ordinaux quelconques avec exactement les même définitions ($\mathrm{mex}\, E$ signifiant : le plus petit ordinal n'appartenant pas à E) alors ω^ω est stable pour les lois $\#$ et $@$ et est une clôture algébrique de $\mathbb{F}_2$. Tout cardinal régulier indénombrable est également stable pour les lois en question et est un corps algébriquement clos de caractéristique 2, et l'ordinal ω^ω est le plus petit transcendant.

Corrigé. Si on suppose $b'\#a = a\#b'$ pour tout $b' < b$, et $b\#a' = a'\#b$ pour tout $a' < a$, alors $b\#a = \mathrm{mex}(\{b'\#a : b' < b\} \cup \{b\#a' : a' < a\}) = \mathrm{mex}(\{a\#b' : b' < b\} \cup \{a'\#b : a' < a\}) = a\#b$, et par récurrence ceci prouve que $\#$ est commutative. Pour tout naturel a on a $a\#0 = \mathrm{mex}\{a'\#0 : a' < a\}$, et si $a'\#0 = a'$ pour tout $a' < a$ alors $a\#0 = a$, ce qui prouve par récurrence que $a\#0 = a$ pour tout a. De même on prouve que $a\#b = 0$ si et seulement si $a = b$ en supposant le résultat vrai en remplaçant a par un $a' < a$ ou en remplaçant b par un $b' < b$: on a alors $\mathrm{mex}(\{a'\#b : a' < a\} \cup \{a\#b' : b' < b\})$ qui est nul si et seulement si aucun des $a'\#b$ et des $a\#b'$ n'est nul (par la définition du mex), c'est-à-dire si et seulement si aucun $a' < a$ n'est égal à b et aucun $b' < b$ égal à a, ce qui signifie clairement $a = b$.

Prouvons maintenant l'associativité : on veut prouver $a\#(b\#c) = (a\#b)\#c$ en supposant ceci vrai en remplaçant a par $a' < a$ ou b par $b' < b$ ou c par $c' < c$. Mais si $e < a\#(b\#c)$, alors soit $e = a'\#(b\#c) = (a'\#b)\#c$ pour un $a' < a$, soit $e = a\#d'$ où $d' < b\#c$ donc $d' = b'\#c$ pour un $b' < b$ ou $d' = b\#c'$ pour un $c < c'$, et dans le premier cas $e = a\#(b'\#c) = (a\#b')\#c$ et dans le second $e = a\#(b\#c') = (a\#b)\#c'$; or toutes ces quantités ($(a'\#b)\#c$ pour $a' < a$, $(a\#b')\#c$ pour $b' < b$ et $(a\#b)\#c'$ pour $c' < c$) sont distinctes de $(a\#b)\#c$ (en utilisant le fait que, trivialement d'après la définition, l'application $x \mapsto x\#d$ est injective pour tout $d \in \mathbb{N}$). Ceci prouve donc que tout $e < a\#(b\#c)$ est différent de $(a\#b)\#c$ donc que $a\#(b\#c) \leq (a\#b)\#c$, mais l'inégalité réciproque se voit exactement de la même manière. D'où l'associativité de $\#$.

La commutativité de $@$, et le fait que $a@0 = 0$ et que $a@1 = a$ sont des récurrences faciles.

Prouvons que $@$ est distributive sur $\#$: on veut prouver que $a@(b\#c) = (a@b)\#(a@c)$ en supposant ceci vrai en remplaçant a par $a' < a$ ou b par $b' < b$ ou c par $c' < c$. Mais si $e < a@(b\#c)$, on peut écrire $e = (a'@(b\#c))\#(a'@d')\#(a@d')$ pour un $a' < a$ et un

$d' < b\#c$ qui s'écrit lui-même soit $d' = b'\#c$ avec $b' < b$ soit $d' = b\#c'$ avec $c' < c$. Supposons la première possibilité (la seconde étant absolument semblable) : on a alors $e = (a'@b)\#(a'@c)\#(a'@b')\#(a'@c)\#(a@b')\#(a@c) = (a'@b)\#(a'@b')\#(a@b')\#(a@c)$ et comme $(a'@b)\#(a'@b')\#(a@b') \neq (a@b)$, on a $e \neq (a@b)\#(a@c)$. Ceci prouve $a@(b\#c) \leq (a@b)\#(a@c)$. Dans l'autre sens, si $e < (a@b)\#(a@c)$, supposons par exemple $e = d'\#(a@c)$ avec $d' < a@b$ donc on peut écrire $d' = (a'@b)\#(a'@b')\#(a@b')$ et alors $e = (a'@b)\#(a'@b')\#(a@b')\#(a@c) = (a'@(b\#c))\#(a'@(b'\#c))\#(a@(b'\#c)) \neq a@(b\#c)$, ce qui prouve l'inégalité dans l'autre sens. D'où la distributivité.

Prouvons l'associativité de @, toujours en procédant par récurrence : si $e < a@(b@c)$, alors en utilisant la distributivité qu'on vient de prouver, il existe $a' < a$, $b' < b$ et $c' < c$ tels que $e = a'@(b@c)\#a'@(b'@c)\#a'@(b'@c')\#a'@(b@c')\#a@(b'@c)\#a@(b'@c')\#a@(b@c')$. Par hypothèse de récurrence, $e = (a'@b)@c\#(a'@b')@c\#(a'@b')@c'\#(a'@b)@c'\#(a@b')@c\#(a@b')@c'\#(a@b)@c' = d'@c\#d'@c'\#(a@b)@c'$ où $d' = (a'@b)\#(a'@b')\#(a@b')$ donc $d \neq a@bx$, donc $e \neq (a@b)@c$ (car $e\#((a@b)@c) \neq 0$). On a ainsi prouvé $a@(b@c) \leq (a@b)@c$, et l'autre inégalité est rigoureusement semblable.

Si $a@b = 0$, cela signifie qu'aucun $(a'@b)\#(a'@b')\#(a@b')$ n'est nul pour $a' < a$ et $b' < b$. Mais comme il est clairement nul pour $a' = 0$ et $b' = 0$, c'est que $a = 0$ et $b = 0$.

Montrons que l'écriture binaire de $a\#b$ s'obtient en prenant les puissances de 2 qui interviennent dans l'écriture binaire de a ou dans celle de b mais pas celles qui interviennent dans les deux (si on veut, le $\#$ est l'opération « ou exclusif » sur les écritures binaires). De nouveau, on procède par récurrence en supposant que la propriété est vraie en remplaçant a par $a' < a$ ou b par $b' < b$. L'hypothèse de récurrence nous assure que a et b sont chacun somme de nim des puissances de deux distinctes dont ils sont somme. S'il y a une puissance de deux commune entre ces deux écritures, on peut l'éliminer (puisque $c\#c = 0$ pour tout c, comme on l'a vu) et l'hypothèse de récurrence donne le résultat. On est donc ramené au cas où a et b n'ont aucune puissance de 2 commune dans leur écriture binaire, et il s'agit de prouver que $a\#b = a + b$. Or si $a' < a$, manifestement $a'\#b \neq a + b$ (c'est clair sur les écritures binaires) et si $b' < b$ de même $a\#b' \neq a+b$, ce qui prouve déjà $a\#b \leq a+b$. Enfin, si $c' < a+b$, en considérant la plus haute puissance de 2 qui est présente dans $a + b$ mais non dans c', disons pour fixer les idées qu'elle est dans a (et pas dans b), on voit aisément qu'on peut trouver $a' < a$ tel que $c' = a'\#b$, donc on a bien $a\#b = a + b$. Ce qui conclut la démonstration du fait annoncé.

Bon, je craque. On a $2^{2^r}@2^{2^s} = 2^{2^r+2^s}$ si $r \neq s$ et plus généralement $2^i@2^j = 2^{i+j}$ si i et j n'ont aucune puissance de 2 commune dans leur écriture binaire, et $2^{2^r}@2^{2^r} = 2^{2^r} + 2^{2^r-1}$ (ce $+$ est aussi un $\#$) : de nouveau, on utilise des récurrences pour le prouver. Ces formules permettent de calculer le produit de nim de deux entiers quelconques, et manifestement si tous deux sont inférieurs à 2^{2^r}, leur produit de nim, comme leur somme de nim, l'est aussi. Donc les entiers de 0 à $2^{2^r} - 1$ forment un anneau intègre fini, c'est-à-dire un corps fini, sous les opérations définies, donc c'est bien $\mathbb{F}_{2^{2^r}}$.

Pour le jeu de nim de dimension 2, appelons « fonction de Grundy » d'une configuration la somme de nim des $a@b$ pour tous les couples (a, b) tels que le pion correspondant soit noir. Si la fonction de Grundy est non nulle, quel que soit le coup joué par un joueur, elle devient non nulle, car on a retourné le pion (a, b) de noir à blanc, donc remplacé $a@b$ par $(a'@b)\#(a'@b')\#(a@b')$ pour $a' < a$ la ligne de l'autre pion retourné sur la même colonne ($a' = 0$ si on n'a pas utilisé cette possibilité) et $b' < b$ la colonne de l'autre pion retourné sur la même ligne ($b' = 0$ sinon). Inversement, si la fonction de Grundy de la configuration était non nulle, il existe un moyen de jouer pour la rendre nulle : comme la somme de nim des $a@b$ est non nulle, il y a moyen en en remplaçant un par $c' < a@b$, de la rendre nulle, et on peut obtenir $c' < a@b$ sous la forme $(a'@b)\#(a'@b')\#(a@b')$ par définition de @, donc on joue à retourne le pion (a, b) ainsi qu'éventuellement les pions (a', b), (a', b') et (a, b') lorsque leurs coordonnées sont non nulles. Enfin, la configuration finale (tous les pions sont blancs) a manifestement une fonction de Grundy nulle. La stratégie gagnante consiste donc à jouer de façon à annuler la fonction de Grundy après son coup : si elle est non nulle initialement, le premier joueur a une stratégie gagnante (annuler la fonction de Grundy, de sorte que le second joueur doit la faire devenir non nulle), et si elle est nulle initialement, c'est le second joueur qui

a une stratégie gagnante (le premier joueur devant faire devenir non nulle la fonction de Grundy).

Pour la dernière question, enfin, on peut commencer par remarquer que toutes les démonstrations effectuées par récurrence pour prouver que les opérations $\#$ et $@$ définissent une structure d'anneau sont encore valables par induction transfinie. L'existence de l'inverse ou la clôture algébrique sont du même ordre : le point essentiel est simplement de montrer que ω^ω est stable par les opérations (c'est le plus petit transcendant). ✓

Motivations : L'exercice 1 est classique et à connaître. Il faut d'ailleurs remarquer la similarité entre le fait que la fraction des polynômes unitaires de degré k sur $\mathbb{F}_q$ qui sont irréductible soit environ $\frac{1}{k}$ et le théorème classique des nombres premiers. L'exercice 2 est lui aussi un grand classique. Il exprime le fait, dans la terminologie introduite par Lang, que les corps finis sont des corps C_1. Le théorème 3 n'est pas moins classique. Il exprime le fait que le groupe de Brauer d'un corps fini est nul. En principe, il devrait être possible de déduire directement un résultat de l'autre (tout corps C_1 a un group de Brauer nul), mais, en pratique, cela donne une démonstration probablement plus compliquée. L'exercice 4 est ultra-classique, et Gauß (qui en a trouvé pas moins de douze démonstrations différentes) l'appelait le « théorème d'or ». L'exercice 5 n'est pas très classique, mais il est amusant. L'exercice 6 n'est pas classique du tout, c'est un craquage de ma part. On trouvera tout plein de choses dans cette ligne d'idées dans le livre *On Numbers and Games* de J. H. Conway.