Corps finis

Plan

- régler la question de la commutativité: le mieux est de prendre comme définition qu'un corps est commutatif et de placer plus loin qu'une algèbre à division finie est commutative;
- pour l'unicité et pour les notations, il est agréable de d'admettre l'existence d'une clôture algébrique (propriété générale qui pourrait être prouvée dans un cours sur les corps), de sorte qu'il y a une unique extension de degré donné d de $\mathbb{F}_p$ plongée dans cette clôture algébrique $\bar{\mathbb{F}}_p$ fixée à l'avance une fois pour toute, que l'on note alors $\mathbb{F}_{p^d}$ (noter qu'ici corps de rupture= corps de décomposition). On pourra alors noter que $\bar{\mathbb{F}}_p = \bigcup_n \mathbb{F}_{q^{n!}}$. Si cette solution ne vous satisfait pas, vous pouvez faire la proposition classique d'existence et unicité à isomorphisme près d'une extension de degré d de $\mathbb{F}_p$ puis dans la foulée vous construisez $\bar{\mathbb{F}}_p = \bigcup_n \mathbb{F}_{q^{n!}}$ en précisant bien que vous prenez à chaque cran $\mathbb{F}_{q^{n!}}$ une extension de $\mathbb{F}_{q^{(n-1)!}}$. Par la suite on considère cette clôture algébrique et on note $\mathbb{F}_{p^d}$ l'unique extension de degré d contenue dans $\bar{\mathbb{F}}_p$;
- il faut donner des exemples: $\mathbb{F}_4$, $\mathbb{F}_8$, $\mathbb{F}_9$;
- donner les règles d'inclusion $\mathbb{F}_q \subset \mathbb{F}_{q'}$ si et seulement si $q = p^r$ et $q' = p^{rn}$;
- $\mathbb{F}_q^\times$ est cyclique;
- parler des groupes finis $PGL_2(\mathbb{F}_2)$, $PGL_2(\mathbb{F}_3)$, $PSL_2(\mathbb{F}_3)$ et $PGL_2(\mathbb{F}_5)$; donner le cardinal de $GL_n(\mathbb{F}_q)$ voir des groupes orthogonaux; le p-sous-groupe de Sylow de $GL_n(\mathbb{F}_q)$;
- faire un paragraphe sur les polynômes: en utilisant le critère que P de degré n est irréductible si et seulement s'il n'a pas de racines dans toutes les extensions de degré inférieure ou égale à $n/2$. Ici c'est particulièrement simple car il y a une unique extension de degré donné de $\mathbb{F}_q$ plongée dans $\bar{\mathbb{F}}_q$.
- introduire le Frobenius, on pourra aussi faire la théorie de Galois;
- on peut aussi parler de codes linéaires et notamment des codes cycliques;
- le solitaire avec l'utilisation de $\mathbb{F}_4$;
- Berlekamp;
- dans la loi de réciprocité quadratique, le symbole de Legendre est un élément de $\mathbb{Z}$.

Développements

- réciprocité quadratique;
- nombre de polynômes irréductibles sur $\mathbb{F}_q$;
- théorie de Galois,
- le théorème de Dirichlet faible;
- Wedderburn
- Etude de la réduction modulo p des polynômes cyclotomiques;
- codes linéaires cycliques;
- Chevalley-Warning

Questions

- $\mathbb{F}_4$ ou $\mathbb{F}_9$;
- factorisation de X^9+2X+1 sur $\mathbb{F}_3$; X^5+X+1 sur $\mathbb{F}_2$, X^5-X+1 sur $\mathbb{F}_5$;
- donner par exemples tous les polynômes de degré 4 sur $\mathbb{F}_2$ puis tous ceux de degré 2 sur $\mathbb{F}_4$ et faire le lien;
- parmi les polynômes irréductibles sur $\mathbb{F}_p$ de degré n, il y a les primitifs au sens où une, et donc toutes leurs racines en utilisant le Frobenius, sont des générateurs du groupe multiplicatif: ce sont exactement les diviseurs de $\Phi_{q-1,\mathbb{F}_p}(X)$;
- le calcul du corps de décomposition de X^n-1 permet de prouver le théorème de Dirichlet faible;
- il existe une infinité de $p\equiv 1 \mod 2^n$;
- loi de réciprocité quadratique; trouver p tel que $(\frac{-5}{p})=1$, ou $(\frac{3}{p})=1$ (en déduire qu'il existe une infinité de $p\equiv 1 \mod 12$;
- soit n qui n'est pas de la forme $2^e p^r$ avec $e=0,1$; alors $\Phi_n(X)$ est irréductible sur $\mathbb{Z}$ et réductible modulo tout p premier; on peut aussi étudier la réduction modulo p des polynômes cyclotomiques;
- étant donné un polynôme P irréductible sur $\mathbb{F}_q$ et de degré n, comment se décompose-t-il sur $\mathbb{F}_{q^m}$; on pourra demander d'abord le cas $n=6$, $m=3$.
- Soit n un entier tel que pour tout p premier sauf éventuellement un nombre fini, n est un carré modulo p. Montrer que n est un carré dans $\mathbb{N}$.

Exercices corrigés

Exercice 1. *Montrer les isomorphismes suivant et donner un générateur du groupe des inversibles des corps en question :*

(i) $\mathbf{F}_4 \simeq \mathbf{F}_2[X]/(X^2+X+1)$ *;*

(ii) $\mathbf{F}_8 \simeq \mathbf{F}_2[X]/(X^3+X+1)$ *;*

(iii) $\mathbf{F}_{16} \simeq \mathbf{F}_2[X]/(X^4+X+1)$ *; donner dans cet isomorphisme l'image de* $\mathbf{F}_4 \subset \mathbf{F}_{16}$ *et en déduire* $\mathbf{F}_{16} \simeq \mathbf{F}_2[X,Y]/(Y^2+Y+1, X^2+X+Y)$.

(iv) $\mathbf{F}_9 \simeq \mathbf{F}_3[X]/(X^2+X-1)$.

Preuve : (i) On vérifie rapidement que X^2+X+1 n'a pas de racines dans $\mathbb{F}_2$, étant de degré 2 il y est alors irréductible de sorte que $\mathbb{F}_2[X]/(X^2+X+1)$ est un corps, une extension de degré 2 de $\mathbb{F}_2$ et donc isomorphe à $\mathbb{F}_4$ qui par convention est **le** corps de cardinal 4 contenu dans une clôture algébrique $\bar{\mathbb{F}}_2$ de $\mathbb{F}_2$ fixée une fois pour toute. Comme $\mathbb{F}_4^\times \simeq \mathbb{Z}/3\mathbb{Z}$, tout élément autre que $0,1$ est un générateur de $\mathbb{F}_4^\times$, soit X et $X+1$.

(ii) De même, on vérifie que X^3+X+1 n'a pas de racines dans $\mathbb{F}_2$; étant de degré 3 il est alors irréductible sur $\mathbb{F}_2$ de sorte que $\mathbb{F}_2[X]/(X^3+X+1)$ est un corps de cardinal 8 et donc isomorphe à $\mathbb{F}_8$. Comme $\mathbb{F}_8^\times \simeq \mathbb{Z}/7\mathbb{Z}$ tout élément autre que $0,1$ est un générateur du groupe des inversibles, par exemple X.

(iii) Encore une fois X^4+X+1 n'a pas de racines sur $\mathbb{F}_2$ mais cela ne suffit pas pour conclure à son irréductibilité; il nous faut montrer que X^4+X+1 n'a pas de racines dans $\mathbb{F}_4$. Soit donc $x\in\mathbb{F}_4$ n'appartenant pas à $\mathbb{F}_2$; on a alors $x^3=1$ de sorte que $x^4+x+1=x+x+1=1\neq 0$. Ainsi X^4+X+1 n'a pas de racines dans les extensions de degré $\leq 4/2$ de $\mathbb{F}_2$ et est donc irréductible sur $\mathbb{F}_2$ de sorte que $\mathbb{F}_2[X]/(X^4+X+1)$ est un corps de cardinal 16 qui est donc isomorphe à $\mathbb{F}_{16}$.

Pour savoir si X est un générateur du groupe multiplicatif, il suffit de vérifier qu'il n'est pas d'ordre 3 ou 5. Or dans la base $1, X, X^2, X^3$, $X^3-1\neq 0$ et $X^5-1=X^2+X+1\neq 0$.

On cherche les éléments de $\mathbb{F}_4$ autres que $0,1$, i.e. des éléments d'ordre 3. Un candidat naturel est $X^5=X^2+X=:\chi$, on a alors $\chi^2=X^4+X^2$ et $\chi^2+\chi+1=0$ et $\chi^3=1$ de sorte que le sous ensemble $\{0,\chi,\chi^2,\chi^3\}$ de $\mathbb{F}_{16}$ correspond au sous-corps $\mathbb{F}_4$. En outre $X^2+\chi X+1$ n'a pas de racines dans $\mathbb{F}_2[\chi]$ et il y est donc irréductible de sorte que $\mathbb{F}_{16}\simeq\mathbb{F}_2[X,Y]/(Y^2+Y+1, X^2+YX+1)$.

(iv) A nouveau X^2+X-1 n'a pas de racines dans $\mathbb{F}_3$, il y est donc irréductible et $\mathbb{F}_9 \simeq \mathbb{F}_3[X]/(X^2+X-1)$. En outre $\mathbb{F}_9^\times \simeq \mathbb{Z}/8\mathbb{Z}$ de sorte qu'il y a $\psi(8)=4$ générateurs et donc 4 non générateurs. On a $X^4=(X-1)^2=X^2-2X+1=-3X+2=-1$ et X est un générateur de $\mathbb{F}_9^\times$.

Exercice 2. *On dira d'une extension de corps $k \subset \bar{k}$ qu'elle est une clôture algébrique si:*

(a) tout élément $x \in \bar{k}$ est algébrique sur k, i.e. il existe une polynôme $P \in k[X]$ tel que $P(x)=0$;

(b) tout polynôme $P \in \bar{k}[X]$ est totalement décomposé dans $\bar{k}$.

Pour tout n, soit $\mathbf{F}_{p^{n!}}$ une extension de degré n de $\mathbf{F}_{p^{(n-1)!}}$. Montrez alors que $\bar{\mathbb{F}}_p := \bigcup_{n>1} \mathbb{F}_{p^{n!}}$ est une cloture algébrique de $\mathbf{F}_p$.

Preuve : Evidemment $\bigcup_{n=1}^N \mathbb{F}_{p^{n!}} = \mathbb{F}_{p^{N!}}$ de sorte que $k=\bigcup_{n=1}^\infty \mathbb{F}_{p^{n!}}$ est une réunion croissante de corps et est donc un corps; en effet pour $x,y \in k$, il existe n tels que $x,y \in \mathbb{F}_{p^{n!}}$ et $x+y, xy$ sont définis dans $\mathbb{F}_{p^{n!}}$. Il est en outre immédiat que k est algébrique sur $\mathbb{F}_p$ car tout $x \in k$ est un élément d'un $\mathbb{F}_{p^{n!}}$ pour n assez grand. Il reste alors à voir que k est algébriquement clos; soit donc $P(X) \in k(X)$ irréductible et soit $\mathbb{F}_{p^m}$ une extension contenant les coefficients de P et soit L un corps de rupture de P dans $\bar{\mathbb{F}}_p$ sur $\mathbb{F}_{p^m}$; L est alors une extension finie de $\mathbb{F}_{p^m}$ et est donc égale à un certain $\mathbb{F}_{p^r}$ et donc inclus dans $\mathbb{F}_{p^{r!}} \subset k$. Ainsi tout polynôme irréductible sur k est de degré 1 soit k algébriquement clos.

Exercice 3. *(i) Donner tous les polynômes irréductibles de degré inférieur à 4 sur $\mathbf{F}_2$.*

(ii) Quelle est la factorisation sur $\mathbb{F}_4$ d'un polynôme de $\mathbb{F}_2[X]$ irréductible de degré 4?

(iii) Déduire des questions précédentes, le nombre de polynômes irréductibles de degré 2 sur $\mathbf{F}_4$.

(iv) Expliciter les polynômes irréductibles de degré 2 sur $\mathbb{F}_4$.

Preuve : (i) Les polynômes irréductibles de degré 1 sont X et $X-1$; ceux de degré 2 sont tels que $X^4-X=X(X-1)P$ ce qui donne X^2+X+1. Pour ceux de degré 3, on a $X^8-X=X(X-1)P_1P_2$ et on trouve X^3+X+1 et X^3+X^2+1. Enfin pour ceux de degré 4, on a $X^16-X=(X^4-X)Q_1Q_2Q_3$ et on trouve X^4+X+1, $X^4+X^3+X^2+X+1$ et X^4+X^3+1. En effet ceux-ci sont irréductibles car un élément j de $\mathbb{F}_4$ qui n'est pas dans $\mathbb{F}_2$ vérifie $j^3=1$ de sorte qu'il ne peut être racine des polynômes en question.

(ii) Tout polynôme de $\mathbb{F}_2[X]$ de degré 4, irréductible sur $\mathbb{F}_2$, possède une racine dans $\mathbb{F}_{2^4}$ qui est une extension de degré 2 de $\mathbb{F}_4$; on en déduit donc que sur $\mathbb{F}_4$ il se factorise en un produit de 2 polynômes irréductibles de degré 2.

(iii) Les 3 polynômes de degré 4, irréductibles dans $\mathbb{F}_2[X]$ fournissent 6 polynômes de $\mathbb{F}_4[X]$ irréductibles de degré 2; ceux-ci sont distincts deux à deux car les 3 polynômes de degré 4 du départ sont premiers deux à deux dans $\mathbb{F}_2$ et donc dans $\mathbb{F}_4$.

Par ailleurs étant donné un polynôme de $\mathbb{F}_4[X]$ irréductible de degré 2, en le multipliant par son conjugué par l'unique élément non trivial du groupe de Galois de $\mathbb{F}_4 : \mathbb{F}_2$, qui échange j et j^2 avec les notations précédentes, on obtient un polynôme de degré 4 à coefficient dans $\mathbb{F}_2$, car les coefficients sont invariants par le groupe de Galois, et irréductible.

(iv) On note $0,1,j,j^2$ les éléments de $\mathbb{F}_4$ avec $1+j+j^2=0$. Les polynômes de degré 1 sont $X, X-1, X-j, X-j^2$ de produit X^4-X. En ce qui concerne le degré 2, X^4+X+1, $X^4+X^3+X^2+X+1$ et X^4+X^3+1 doivent s'écrire comme le produit de 2 polynôme irréductible de degré sur $\mathbb{F}_4$. On trouve alors $X^4+X+1=(X^2+X+j)(X^2+X+j^2)$, $X^4+X^3+1=(X^2+jX+j)(X^2+j^2X+j^2)$ et $X^4+X^3+X^2+X+1=(X^2+jX+1)(X^2+j^2X+1)$.

Exercice 4. *(1) Le nombre 2 est-il un carré dans $\mathbf{F}_5$? Montrer que X^2+X+1 est irréductible sur $\mathbf{F}_5$.*

(2) Soit $P(X) \in \mathbf{F}_5[X]$ un polynôme unitaire irréductible de degré deux . Montrer que le quotient

$$\frac{\mathbf{F}_5[X]}{(P(X))}$$

est isomorphe au corps $\mathbf{F}_{25}$ et que P a deux racines dans $\mathbf{F}_{25}$.

(3) On note α une racine de X^2+X+1 dans $\mathbf{F}_{25}$. Montrer que tout $\beta \in \mathbf{F}_{25}$ peut s'écrire $a\alpha+b$ avec a et b dans $\mathbf{F}_5$.

(4) Soit $P=X^5-X+1$. Montrer que pour tout $\beta \in \mathbf{F}_{25}$, on a $P(\beta) \neq 0$. En déduire que P est irréductible sur $\mathbf{F}_5$. P est-il irréductible sur $\mathbf{Q}$?

Preuve :

(1) On écrit la table des carrés de $\mathbb{F}_5$, soit

x	0	1	2	-2	-1
x^2	0	1	-1	-1	1

et on remarque que 2 n'est pas un carré dans $\mathbb{F}_5$.

On vérifie rapidement que pour $P(x) := X^2 + X + 1$, $P(0)$, $P(\pm 1)$ et $P(\pm 2)$ ne sont pas nuls de sorte que P n'a pas de racine dans $\mathbb{F}_5$, étant de degré 2 il y est donc irréductible.

(3) Le corps $\mathbb{F}_5[X]/(P(X))$ est de cardinal 25 et donc isomorphe à $\mathbb{F}_{25}$ qui est un corps de décomposition de $X^{25} - X$. Par ailleurs la classe x de X dans $\mathbb{F}_5[X]/(P(X))$ vérifie $P(x) = 0$ de sorte que x est une racine de P qui étant de degré 2, y est alors totalement décomposé. On en déduit alors que P admet deux racines dans $\mathbb{F}_{25}$.

(3) Un isomorphisme $f : \mathbb{F}_5[X]/(X^2 + X + 1) \simeq \mathbb{F}_{25}$ étant fixée, l'image $\alpha \in \mathbb{F}_{25}$ de X par f vérifie alors $\alpha^2 + \alpha + 1 = 0$ et est donc une racine de $X^2 + X + 1$. Le sous-espace vectoriel sur $\mathbb{F}_5$ de $\mathbb{F}_{25}$ engendré par 1 et α est de dimension 2 car $\alpha \notin \mathbb{F}_5$ et est donc égal à $\mathbb{F}_{25}$ de sorte que tout élément $\beta \in \mathbb{F}_{25}$ s'écrit sous la forme $a\alpha + b$ avec $a, b \in \mathbb{F}_5$.

(4) On vérifie rapidement que P n'a pas de racine dans $\mathbb{F}_5$. Soit alors $\beta = a\alpha + b \in \mathbb{F}_{25}$; on a $\beta^5 = a^5\alpha^5 + b^5 = a\alpha^5 + b$. Or on a $\alpha^2 = -\alpha - 1$ soit $\alpha^4 = \alpha^2 + 2\alpha + 1 = \alpha$ et donc $\alpha^5 = \alpha^2 = -\alpha - 1$. Ainsi $\beta^5 - \beta + 1 = \alpha(-a - a) + (b - b - a + 1) \neq 0$ car $\alpha \notin \mathbb{F}_5$ soit P n'a pas de racine dans $\mathbb{F}_{25}$ de sorte qu'il est irréductible sur $\mathbb{F}_5$.

Par ailleurs, P en tant que polynôme de $\mathbb{Z}[X]$ unitaire, y est irréductible. En effet une factorisation $P = QR$ dans $\mathbb{Z}[X]$ induit par réduction modulo 5 une factorisation $\bar{P} = \bar{Q}\bar{R}$ dans $\mathbb{F}_5[X]$. Comme P est unitaire, Q et R le sont aussi, de sorte que $\deg Q = \deg \bar{Q}$ et $\deg R = \deg \bar{R}$; $\bar{P}$ étant irréductible, on en déduit que $\bar{Q}$, ou $\bar{R}$, est un polynôme constant donc, étant unitaire, égal à $\bar{1}$ et donc Q, ou R, est le polynôme constant égal à 1. Ainsi P est irréductible sur $\mathbb{Z}$ et donc irréductible sur $\mathbb{Q}$ d'après le lemme de Gauss.

Exercice 5. *On considère le polynôme $Q(X) = X^9 - X + 1$ sur $\mathbf{F}_3$.*

(a) Montrer que le polynôme Q n'a pas de racines dans $\mathbb{F}_3, \mathbb{F}_9$.

(b) Montrer que $\mathbb{F}_{27} \simeq \frac{\mathbb{F}_3[X]}{(X^3 - X - 1)}$.

(c) Montrer que toute racine $\alpha \in \mathbb{F}_{27}$ du polynôme $X^3 - X - 1$ est une racine du polynôme Q.

(d) Déterminer toutes le racines de Q dans $\mathbb{F}_{27}$.

(e) Factoriser le polynôme Q sur le corps $\mathbb{F}_3$.

Preuve : (a) on vérifie rapidement que Q n'a pas de racine dans $\mathbb{F}_3$. On cherche alors ses racines dans $\mathbb{F}_9$. Pour $a \in \mathbb{F}_9$, on a $a^9 = a$ de sorte que $a^9 - a + 1 = 1$ et donc Q n'a pas de racine dans $\mathbb{F}_9$.

(b) Afin de calculer dans $\mathbb{F}_{27}$, on commence par le décrire concrètement: on vérifie aisément que $X^3 - X - 1$ n'a pas de racines dans $\mathbb{F}_3$ et est donc irréductible sur $\mathbb{F}_3$ et $\mathbb{F}_{27} \simeq \mathbb{F}_3[X]/(X^3 - X - 1)$.

(c) Soit alors $\alpha \in \mathbb{F}_{27}$ tel que $\alpha^3 = \alpha + 1$. On a alors $\alpha^9 = \alpha^3 + 1 = \alpha + 2 = \alpha - 1$ et donc finalement α est une racine de Q dans $\mathbb{F}_{27}$ de sorte que Q possède un facteur irréductible de degré 3 sur $\mathbb{F}_3$, à savoir $X^3 - X - 1$, soit $X^9 - X + 1 = (X^3 - X - 1)(X^6 + X^4 + X^3 + X^2 - X - 1)$.

(d) Cherchons de manière générale toutes les racines dans $\mathbb{F}_{27}$; un élément quelconque s'écrit sous la forme $x = a\alpha^2 + b\alpha + c$ avec $a, b, c \in \mathbb{F}_3$. On a alors $x^9 = a\alpha^{18} + b\alpha^9 + c$ avec $\alpha^9 = \alpha - 1$ et donc $\alpha^{18} = \alpha^2 + \alpha + 1$ de sorte que $x^9 - x + 1 = a\alpha + a - b + 1$ ce qui impose $a = 0$ et $b = 1$ soit $x = \alpha, \alpha + 1, \alpha - 1$.

(e) On en déduit alors que $X^6 + X^4 + X^3 + X^2 - X - 1$ n'a pas de racines dans $\mathbb{F}_{27}$ comme il n'en avait pas non plus dans $\mathbb{F}_9$, il est donc irréductible.

Exercice 6. *A quelle condition un polynôme P à coefficients dans $\mathbf{F}_p$ de degré n est-il irréductible sur $\mathbf{F}_{p^m}$? Dans le cas où P est irréductible sur $\mathbf{F}_p$, on donnera des précisions sur les degrés des facteurs irréductibles de P sur $\mathbf{F}_{p^m}$. En particulier pour $n = 5$, donner m minimal tel que tout polynôme de degré 5 à coefficients dans $\mathbf{F}_p$ soit totalement décomposé (resp. possède une racine) sur $\mathbf{F}_{p^m}$.*

Preuve : Si P est réductible sur $\mathbb{F}_p$, il l'est sur toute extension $\mathbb{F}_{p^m}$. Supposons donc P irréductible sur $\mathbb{F}_p$ de sorte que toutes les racines de P, vues dans $\bar{\mathbb{F}}_p$, sont dans $\mathbb{F}_{p^n}$ et aucune n'appartient à un sous-corps strict. On regarde alors P comme un polynôme dans $\mathbb{F}_{p^m}[X]$ dont on se demande s'il est encore irréductible. Il faut regarder s'il possède ou non des racines dans $\mathbb{F}_{p^{mr}}$ pour $r \leq n/2$ et donc si $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^{mr}}$, soit n divise mr ce qui est possible si et seulement si n et m ne sont pas premiers entre eux. En outre en notant $d = n \wedge m$, les facteurs irréductibles sont alors de degré r un multiple de n/d.

Pour $n = 5$, la décomposition en facteur irréductible donne en prenant les degrés les décompositions suivantes de 5: $5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1$. Si on veut être sur d'avoir toutes les racines (resp. au moins une racine) il faut donc se placer dans $\mathbb{F}_{p^{60}}$ (resp. $\mathbb{F}_{p^{10}}$) avec $60 = 5.4.3$ (resp. $10 + 5.2$).

Exercice 7. *Théorie de Galois des corps finis et version faible du théorème de Dirichlet: Soit p un nombre premier et n un entier premier avec p. On pose $q = p^r$.*

(1) Décrire le groupe de Galois de l'extension $\mathbb{F}_{q^n} : \mathbb{F}_q$ et expliciter la théorie de Galois, i.e. montrer que l'application qui à un sous-groupe H de $gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$ associe le sous-corps de $\mathbb{F}_{q^n}$ des éléments fixés par tous les éléments de H, est une bijection entre les sous-groupes du groupe de Galois et les extensions intermédiaires $\mathbb{F}_q \subset \mathbf{K} \subset \mathbb{F}_{q^n}$.

(2) Soit $L = Dec_{\mathbb{F}_p}(X^n - 1)$. Montrer que $\mathrm{Gal}(L/\mathbb{F}_p)$ est isomorphe au sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par l'image de p. Montrer que le n-ième polynôme cyclotomique $\Phi_n(X)$ se décompose sur $\mathbb{F}_p$ en un produit de $\phi(n)/k$ facteurs irréductibles distincts, tous de degré k. Quel est cet entier k? En déduire une version faible du théorème de progression arithmétique, i.e. :
pour tout entier n il existe une infinité de nombres premiers p congrus à 1 modulo n.

Preuve : (1) On considère le morphisme de Frobenius

$$\mathrm{Fr}_q : x \in \mathbb{F}_{q^n} \longmapsto x^q \in \mathbb{F}_{q^n}$$

dont on vérifie aisément que c'est un morphisme de corps car $\mathrm{Fr}_q(x+y) = (x+y)^q = x^q + y^q$ et $\mathrm{Fr}_q(xy) = x^q y^q$, qui laisse le corps $\mathbb{F}_q$ invariant car pour tout $x \in \mathbb{F}_q$ on a $x^q = x$. En outre il est immédiat que le groupe engendré par Fr_q est d'ordre n de sorte que $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ est de cardinal supérieur ou égal à n. Pour montrer l'inégalité inverse, soit χ un générateur de $\mathbb{F}_{q^n}^\times$ et soit μ_χ son polynôme minimal unitaire sur $\mathbb{F}_q$; on a alors $\mathbb{F}_{q^n} \simeq \mathbb{F}_q[X]/(\mu_\chi(X))$ de sorte que μ_χ est irréductible de degré n. Ainsi tout élément $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ est déterminée par $\sigma(\chi)$ qui doit être une racine de μ_χ ce qui donne au plus n choix. On en déduit ainsi $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) =< \mathrm{Fr}_q > \simeq \mathbb{Z}/n\mathbb{Z}$.

Un sous-groupe H de $\mathbb{Z}/n\mathbb{Z}$ est de la forme $\mathbb{Z}/r\mathbb{Z}$ pour r un diviseur de n, un générateur étant n/r. On considère alors le sous-groupe de $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ engendré par $\mathrm{Fr}_q^{n/r}$; le sous-corps fixé est alors l'ensemble des éléments x de $\mathbb{F}_{q^n}$ tels que $x^{q^{n/r}} = x$ ce qui correspond au corps $\mathbb{F}_{q^{n/r}} \subset \mathbb{F}_{q^n}$. D'après l'exercice précédent, l'application de la théorie de Galois est bien une bijection.

(2) Le corps L est isomorphe à $\mathbb{F}_{p^r}$ pour un certain r et $\mathrm{Gal}(L/\mathbb{F}_p) \simeq \mathbb{Z}/r\mathbb{Z}$ engendré par Fr_p. En outre on a $L = \mathbb{F}_p[\chi]$ pour $\chi \in L$ une racine primitive n-ième de l'unité. Ainsi un élément $\sigma \in \mathrm{Gal}(L/\mathbb{F}_p)$ est déterminé par $\sigma(\chi)$ qui doit être une racine primitive n-ième de l'unité et donc de la forme χ^k pour $k \in (\mathbb{Z}/n\mathbb{Z})^\times$. On obtient ainsi une application injective naturelle

$$\sigma \in \mathrm{Gal}(L/\mathbb{F}_p) \longmapsto k \in (\mathbb{Z}/n\mathbb{Z})^\times$$

l'image étant le groupe engendré par la classe de p. Ainsi r est l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$.

Soit $\bar{\Phi}_n(X) = P_1 \cdots P_s$ la décomposition en irréductibles de la réduction modulo p de Φ_n. Soit χ une racine de P_1 de sorte que $L = \mathbb{F}_p[\chi]$ et donc P_1 est le polynôme minimal de χ sur $\mathbb{F}_p$ et donc $\deg P_1 = [L : \mathbb{F}_p]$. En conclusion tous les P_i sont de même degré $[L : \mathbb{F}_p]$ et donc $s = \frac{\psi(n)}{[L:\mathbb{F}_p]}$ où l'on rappelle que $[L : \mathbb{F}_p]$ est l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$.

Ainsi $p \equiv 1 \mod n$ est équivalent à demander que $\bar{\Phi}_n$ est totalement décomposé sur $\mathbb{F}_p$ ce qui on vient de le voir, est équivalent à demander que $\bar{\Phi}_n$ a une racine dans $\mathbb{F}_p$. Soit donc p premier divisant $\Phi_n(N!) \equiv 1 \mod N!$ soit $p > N$ et $p \equiv 1 \mod n$ car $\bar{\Phi}_n$ a pour racine $\bar{N}!$. On vient donc de montrer une version faible du théorème de

progression arithmétique dont l'énoncé fort est que pour tout a premier avec n, il existe une infinité de premiers congrus à a modulo n, ceux-ci se répartissant de manière uniforme en un sens que l'on ne précise pas ici, sur les $a \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Exercice 8. *(i) Montrer que X^4+1 est irréductible sur $\mathbb{Z}$ et réductible modulo tout nombre premier p. (Indication : montrer que pour tout nombre premier impair p, le polynôme X^4+1 a une racine dans le corps $\mathbb{F}_{p^2}$.*

(ii) Soit n un entier ne s'écrivant pas sous la forme p^α ou $2p^\alpha$ avec p premier impair. On sait que le n-ième polynôme cyclotomique Φ_n est irréductible sur $\mathbb{Z}$. Montrer que Φ_n est réductible modulo tout nombre premier.

Preuve : (i) Le polynôme X^4+1 est le huitième polynôme cyclotomique Φ_8 qui est irréductible. On peut aussi le voir directement en considérant $\Phi_8(X+1)$ qui est un polynôme d'Eisenstein pour 2.

Modulo 2, on a $X^4+1=(X+1)^4$ et pour $p \neq 2$, $\mathbb{F}_{p^2}^\times$ est cyclique d'ordre p^2-1 qui est divisible par 8. Soit alors $x \in \mathbb{F}_{p^2}^\times$ d'ordre 8, on a $x^8=(x^4)^2=1$ et $x^4 \neq 1$ soit $x^4=-1$ de sorte que Φ_8 a une racine dans $\mathbb{F}_{p^2}$ et donc Φ_8 est réductible modulo p.

(ii) Avec les hypothèses de l'énoncé $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique. D'après loc. cit., la réduction modulo p de Φ_n est un produit de polynômes irréductibles qui ont tous le même degré à savoir l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Ainsi Φ_n est irréductible modulo p si et seulement si p engendre $(\mathbb{Z}/n\mathbb{Z})^\times$ ce qui ne se peut pas si ce dernier groupe n'est pas cyclique.

Remarque: On a ainsi une famille d'exemples de polynômes irréductibles sur $\mathbb{Z}$ et réductible modulo tout premier p.

Exercice 9. *Montrez que $PGL_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$ et $PGL_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$.*

Preuve: (a) On fait agir $PGL_2(\mathbb{F}_3)$ sur $\mathbb{P}^1(\mathbb{F}_3)$ naturellement, i.e. $M.\overline{\binom{x}{y}} := \overline{M\binom{x}{y}}$; $\mathbb{P}^1(\mathbb{F}_3)$ étant de cardinal 4, on en déduit un morphisme $PGL_2(\mathbb{F}_3) \longrightarrow \mathfrak{S}_4$ qui est injectif; en effet si pour tout vecteur v de $\mathbb{F}_3^2$, v est vecteur propre pour une valeur propre λ_v de M, c'est un exercice classique d'algèbre linéaire de montrer que λ_v est indépendant de v et donc $M=\lambda Id$. Or $PGL_2(\mathbb{F}_3)$ est de cardinal $(9-1)(9-3)/2=24$, d'où le résultat.

(b) On fait de même agir $PGL_2(\mathbb{F}_5)$ sur $\mathbb{P}^1(\mathbb{F}_5)$ et on obtient ainsi un morphisme injectif $PGL_2(\mathbb{F}_5) \longrightarrow \mathfrak{S}_6$. En outre $PGL_2(\mathbb{F}_5)$ est de cardinal 120; le résultat découle alors du fait général suivant: tout sous-groupe d'indice n de $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$. (cf. td 6)

□

Exercice 10. *Montrer l'existence d'une infinité de nombres premiers $p \equiv -1 \mod 12$.*

Preuve : Si p divise a^2-3b^2 et p premier avec b alors 3 est un carré modulo p. Or on a $(\frac{3}{p})=(\frac{p}{3})(-1)^{(p-1)/2}$ et donc 3 est un carré modulo p dans les deux situations suivantes:

- $(\frac{p}{3})=(-1)^{(p-1)/2}=1$ soit $p \equiv 1 \mod 3$ et $p \equiv 1 \mod 4$ soit $p \equiv 1 \mod 12$;
- $(\frac{p}{3})=(-1)^{(p-1)/2}=-1$ soit $p \equiv -1 \mod 3$ et $p \equiv -1 \mod 4$ soit $p \equiv -1 \mod 12$;

Soit alors $N=3(n!)^2-1$; tout diviseur premier p de N est alors congru à ± 1 modulo 12 et supérieur à n de sorte que par hypothèse, $p \equiv 1 \mod 12$. On en déduit alors que $N \equiv 1 \mod 12$ ce qui n'est pas car $N \equiv -1 \mod 12$.

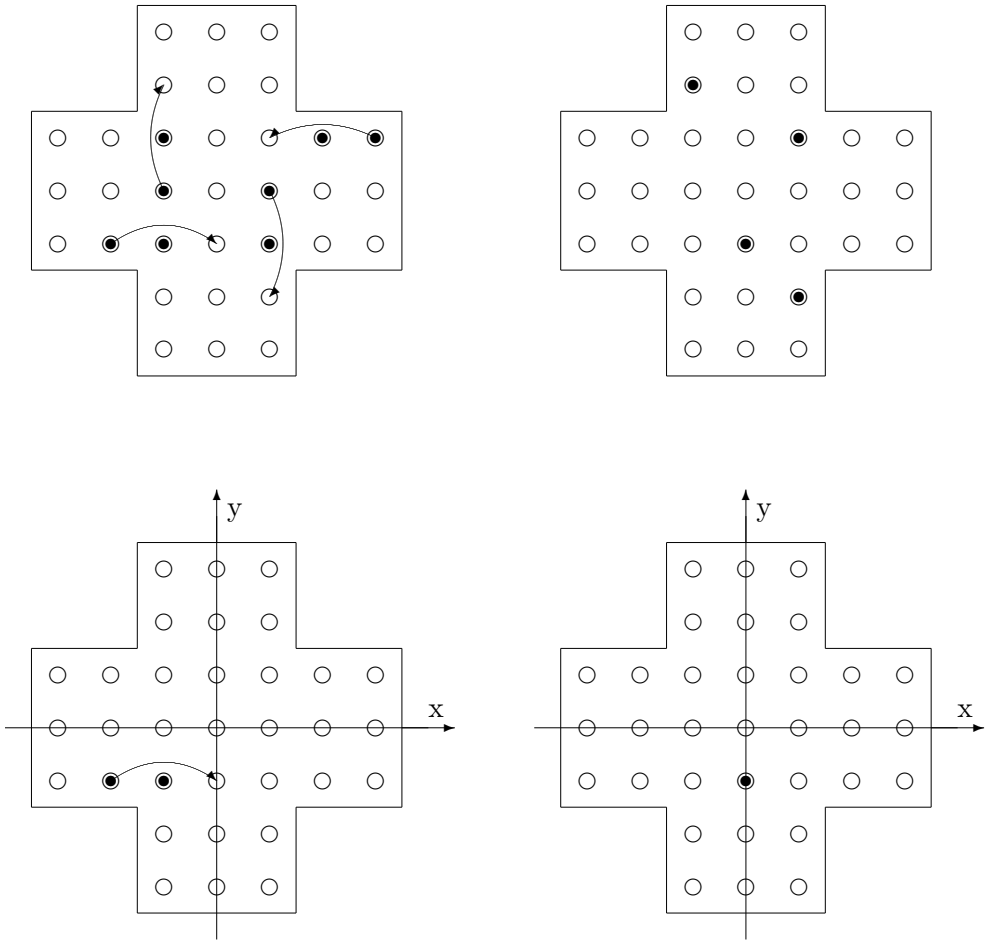
Exercice 11. *Le jeu du solitaire se joue sur un plateau disposant de 33 réceptacles (cercle vide) dans lesquels il peut y avoir des billes notés avec un cercle plein. A chaque étape on peut faire passer une bille au dessus d'une autre sur un axe vertical ou horizontal, pourvu que le réceptacle suivant soit vide, comme dans la figure suivante*

Soit alors O placé au centre du plateau et un repère (O,x,y) comme dans la figure suivante et pour une configuration $\mathcal{C}$ quelconque de billes sur le plateau on introduit

$$\alpha_{\mathcal{C}} := \sum_{(x,y)\in\mathcal{C}} j^{x+y} \in \mathbb{F}_4 \quad \beta_{\mathcal{C}} := \sum_{(x,y)\in\mathcal{C}} j^{x-y} \in \mathbb{F}_4$$

où j est un générateur de $\mathbb{F}_4^\times$.

(1) Montrer que (α,β) est un invariant du jeu.



(2) Habituellement le jeu consiste à partir d'une configuration où l'on place des billes dans tous les réceptacles sauf un seul disons (x_0, y_0) et à arriver à la configuration où tous les réceptacles sont vides sauf celui (x_0, y_0). Montrer qu'effectivement les deux configurations précédentes, possèdent les mêmes invariants (α, β).

(3) Partant de la configuration suivante, montrer qu'il est impossible d'arriver à une configuration où il n'y aurait qu'une seule bille sur le plateau.

Preuve :

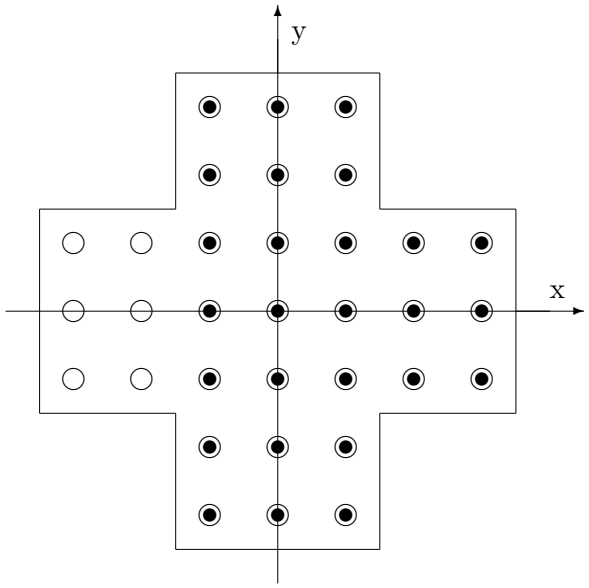
(1) Prenons par exemple le mouvement élémentaire de la figure (11). Dans le plateau de gauche on a $\alpha = j^{x_0+y_0}(1+j)$ (resp. $\beta = j^{x_0-y_0}(1+j)$) alors que dans le plateau de droite on a $\alpha = j^{x_0+y_0}.j^2$ (resp. $\beta = j^{x_0-y_0}j^2$), avec $(x_0, y_0) = (-2, -1)$. Le résultat découle alors de l'égalité $1 + j = j^2$ dans $\mathbb{F}_4$ (on rappelle que dans $\mathbb{F}_4$, on a $1 = -1$). Les autres mouvements élémentaires se traitent de manière strictement identique.

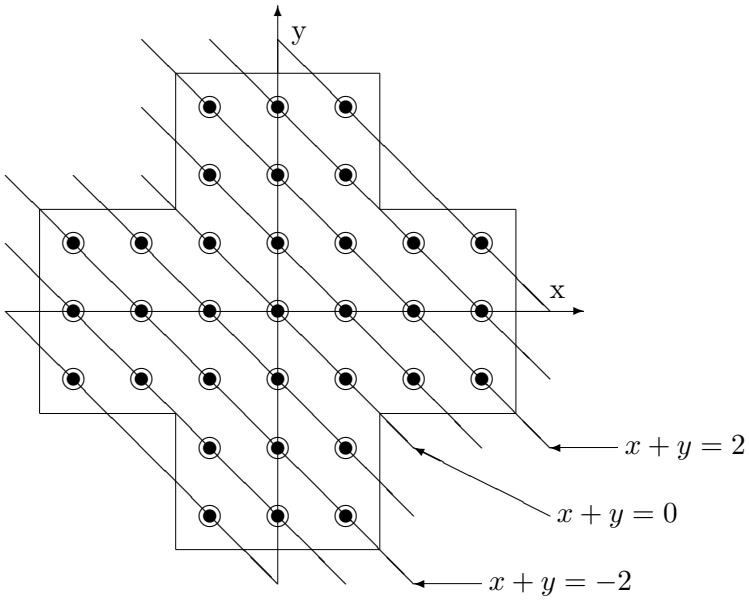
(2) Commençons par calculer (α, β) pour la configuration où tous les réceptacles contiennent une bille. La configuration étant invariante par la réflexion d'axe (Oy), on a $\alpha = \beta$, calculons donc α. Pour cela on propose de sommer sur les droites $x + y$ constantes, de sorte que ne contribuent que les droites où il y a un nombre impair de billes, ce qui donne $\alpha = j^0 + j^2 + j^{-2} = 0$, comme on le voit sur la figure suivante.

Notons alors avec un indice *tot* (resp. $\mathcal{C}_0$, resp. 0) ce qui fait référence à la configuration où tous les réceptacles sont remplis (resp. tous sauf en (x_0, y_0), resp aucun sauf en (x_0, y_0)). On a ainsi $(\alpha_{tot}, \beta_{tot}) = (\alpha_{\mathcal{C}_0}, \beta_{\mathcal{C}_0}) + (\alpha_0, \beta_0) = (0, 0)$ de sorte que $(\alpha_{\mathcal{C}_0}, \beta_{\mathcal{C}_0}) = (\alpha_0, \beta_0)$.

(3) On calcule comme précédemment les invariant (α, β) ce qui donne $(0, 0)$ qui ne peut pas être de la forme $(j^{x_0+y_0}, j^{x_0-y_0})$.

Exercice 12. *Soit n un entier tel que pour tout p premier sauf éventuellement un nombre fini, n est un carré modulo p. Montrer que n est un carré dans $\mathbb{N}$.*





Preuve : Soit $p_1, \cdots, p_n$ tels que pour tout $p \neq p_i$, n est un carré modulo p. Supposons n sans facteur carré et distinct de $\pm 1, \pm 2$. On écrit $n = hl_1 \cdots l_k$ avec $h \in \{\pm 1, \pm 2\}$ et où les l_i sont premiers impairs distincts ($k \geq 1$). Il existe un entier naturel a tel que:

$$a \equiv 1 \mod 8p_1 \cdots p_n l_1 \cdots l_{k-1} \text{ et } a \equiv r \mod l_k$$

D'après la loi de réciprocité quadratique on a

$$(\frac{n}{a}) = (\frac{l_1 \cdots l_k}{a}) = \prod_i (\frac{a}{l_i}) = (\frac{1}{l_1}) \cdots (\frac{1}{l_{k-1}})(\frac{r}{l_k}) = -1$$

de sorte que a a un diviseur premier p distinct des p_i tel que $(\frac{n}{p}) = -1$, d'où la contradiction.