Concours Agrégation, Mathématiques générales

Leçon 23- Corps finis. Applications.

Commentaires du jury 2015 : Il s'agit d'une leçon comportant un certain nombre d'attendus. En premier lieu, une construction des corps finis doit être connue. Ensuite, les constructions des corps de petit cardinal doivent avoir été pratiquées. Les injections des divers $\mathbb{F}_q$ doivent être connues. Enfin, les applications des corps finis (y compris pour $\mathbb{F}_q$ avec q non premier !) ne doivent pas être oubliées : citons par exemple l'étude de polynômes à coefficients entiers et de leur irréductibilité. Il sera bon de comprendre l'utilisation des degrés des extensions, et leurs petites propriétés arithmé- tiques amenées par le théorème de la base téléscopique. Un candidat qui étudie les carrés dans un corps fini doit savoir aussi résoudre les équations de degré 2. Le théorème de l'élément primitif, s'il est énoncé, doit pouvoir être utilisé. Les applications sont nombreuses. S'ils sont bien maîtrisées, alors les codes correcteurs peuvent être mentionés.
Commentaires du jury 2016 : Une construction des corps finis doit être connue et une bonne maîtrise des calculs dans les corps finis est indispensable. Les injections des divers F q doivent être connues et les applications des corps finis (y compris pour F q avec q non premier !) ne doivent pas être oubliées : citons par exemple l'étude de polynômes à coefficients entiers et de leur irréductibilité. Le calcul des degrés des extensions et le théorème de la base téléscopique sont incontournables. L'étude des carrés dans un corps fini et la résolution d'équations de degré 2 sont envisageables. S'ils le désirent, les candidats peuvent aller plus loin en détaillant des codes correcteurs.

Bibliographie

[F. M. 1] Fresnel J., Matignon M. *Algèbre et Géométrie* (Hermann 2011)
[F. M. 1'] Errata, https://www.math.u-bordeaux.fr/∼mmatigno/Errata-Alg-Géom.pdf
[F. M. 2] Fresnel J., Matignon M. *Algèbre et Géométrie-81 thèmes pour l'agrégation* (ellipses 2017)
[F. M. 2'] Compléments et errata, https://www.math.u-bordeaux.fr/∼mmatigno/Errata-FM2.pdf
[Fr. F] Fresnel J. *Anneaux* (Hermann 2001)
et
[Se.] Serre J.P. *Cours d'arithmétique* (PUF 1970)

Développements conseillés :

(1) Sur les sous-groupes cycliques de $Gl_n(\mathbb{F}_q)$ d'ordre $q^n - 1$, [F. M. 2] p. 53.
(2) Loi de réciprocité quadratique, [F. M. 1] $n°87$ la preuve de V.A. Lebesgue p. 248.
(3) Loi de réciprocité quadratique via les polynômes cyclotomiques, [F. M. 2] p. 243.
(4) Autour de Berlekamp [F. M. 1] $n°108$ p. 299 partie A. Appliquer l'algorithme au polynôme $X^p - X - 1 \in \mathbb{F}_p[X]$

Exercice 1

(1) Montrer que $P := X^5 + X^2 + 1$ est irréductible dans $\mathbb{F}_2[X]$ et en déduire l'irréductibilité de P dans $\mathbb{Z}[X]$.
(2) Montrer que $P := X^5 - X - 1$ est irréductible dans $\mathbb{F}_3[X]$ et en déduire l'irréductibilité de P dans $\mathbb{Z}[X]$.

Exercice 2 Soit K, un corps commutatif et G un sous-groupe fini du groupe multiplicatif $K^\times = K - \{0\}$ de K, alors G est cyclique.

Preuve.

- On utilise le théorème de structure des groupes abéliens finis.
  Si $|G| > 1$, il existe une suite d'entiers $1 < a_1|a_2|...|a_r$ avec $(G, \times) \simeq (\frac{\mathbb{Z}}{a_1\mathbb{Z}} \times ... \times \frac{\mathbb{Z}}{a_r\mathbb{Z}}, +)$. Il s'agit de montrer que $r = 1$. Puisque $a_r G = \{0\}$, il suit que le cardinal de $\{z \in K \mid z^{a_r}\} = 1$ est $\geq |G| = a_1 a_2 ... a_r$ et d'autre part le nombre de racines dans K du polynôme $X^{a_r} - 1 \in K[X]$ est

inférieur ou égal à son degré parce que le corps K est commutatif (c'est faux pour le corps des quaternions sur $\mathbb{R}$ par exemple). Ainsi $a_1a_2...a_r \leq a_r$ ce qui implique $r = 1$.

- Une variante utilise le lemme clé qui sert à démontrer le théorème de structure des groupes abéliens finis à savoir que si G est un groupe abélien fini il existe $g \in G$ avec $o(g) = ppcm\{o(x) \mid x \in G\}$, voir [Fr. F.] p. 33.
- Une preuve inspirée de la preuve de [Se.] p. 11, pour montrer que le groupe multiplicatif d'un corps fini est cyclique.

  L'idée de base est de considérer la partition de G par l'ordre de ses éléments et d'utiliser la formule classique d'Euler (1) $n = \sum_{d|n} \varphi(d)$.

  On note $n = |G|$ et $\varphi_G(d)$ le nombre d'éléments de G d'ordre d. On a donc (2) $n = |G| = \sum_{d|n} \varphi_G(d)$. Si $\varphi_G(d) \geq 1$ alors $d|n$ et il existe $g \in G$ qui est d'ordre d, ainsi il y a d éléments dans le groupe cyclique $< g >$ et ce sont donc les d racines du polynôme $X^d - 1 \in K[X]$. Il suit que si $g' \in G$ est un élément d'ordre d alors $g' \in < g >$ et donc $\varphi_G(d) = \varphi(d)$, le nombre d'éléments d'ordre d dans le groupe cyclique $< g >$. Ainsi il suit de (1) et (2) que $0 = \sum_{d|n}(\varphi(d) - \varphi_G(d))$ est une somme de nombres positifs et donc en particulier $\varphi_G(n) = \varphi(n) > 0$. Nous avons montré que G qui est d'ordre n contient un élément d'ordre n; il est donc cyclique.

Exercice 3 Existence et unicité à isomorphisme d'un corps fini à $q = p^n$ éléments sans l'utilisation d'une clôture algébrique. Notez que dans [Se.] chap. I, on utilise l'existence d'une clôture algébrique.

On rappelle que les corps finis sont commutatifs (c'est Wederburn).

(1) *Existence*

(a) *Corps de rupture.* Soit K un corps commutatif et $P \in K[X]$, un polynôme irréductible. Montrer que $K_1 := \frac{K[X]}{PK[X]}$ est un corps commutatif, que K s'injecte dans K_1 et qu'il existe $x \in K_1$ avec $P(x) = 0$.

Preuve. Soit $\pi : K[X] \to K_1$, la surjection canonique. Puisque $K \cap PK[X] = \{0\}$, il suit que K s'injecte dans K_1. Si $y = \pi(Q) \in K_1 - \{0\}$, alors P ne divise pas Q et ainsi l'idéal $PK[X] + QK[X]$ est principal et engendré par un diviseur de P et puisque P est irréductible cet idéal est l'idéal (1). Ainsi il existe $U, V \in K[X]$ avec $1 = UP + VQ$ et donc $y\pi(V) = 1$, ainsi K_1 est un corps. Si $x := \pi(X)$, on a $0 = \pi(P(X)) = P(x)$. ///

(b) *Corps de décomposition.* Soit K un corps commutatif et soit $Q \in K[X]$ avec $\deg Q \geq 1$. Déduire de la question précédente l'existence d'un corps L avec une injection de K dans L et tels que Q se factorise dans $L[X]$ en un produit de polynômes de degré 1 (faire une récurrence sur le degré: supposer le résultat vrai pour tout corps K et tout polynôme $Q \in K[X]$ de degré n).

Preuve. Si $\deg Q = 1$, c'est immédiat. Soit donc $Q \in K[X]$ de degré $n + 1$, puisque $K[X]$ est principal, il existe $P \in K[X]$ un diviseur irréductible de Q. Soit K_1 et $x \in K_1$ construits dans la question précédente alors $X - x$ divise Q dans $K_1[X]$. On applique l'hypothèse de récurrence au polynôme $\frac{Q}{X-x} \in K_1[X]$. ///

(c) *Corps fini à $q = p^n$ éléments.* Soit $Q := X^q - X \in \mathbb{F}_p[X]$ et L un corps de décomposition de Q. Montrer que L contient un et un seul corps à $q = p^n$ éléments.

Preuve. Soit K l'ensemble des racines dans L de Q. Puisque le polynôme dérivé $Q' = -1$, il suit que les racines de Q sont simples et donc $|K| = p^n = q$. Notons $F : L \to L$ l'application $F(y) = y^p$. Puisque $F(y + z) = (y + z)^p = \sum_{0 \leq i \leq p} \binom{p}{i} y^i z^{p-i}$ et que $p|\binom{p}{i}$ si $0 < i < p$, il suit que $F(y + z) = F(y) + F(z)$. On vérifie alors que K est un corps. ///

(2) *Existence d'un polynôme irréductible $\in \mathbb{F}_p[X]$ de degré n .*

Soit L, un corps à $q = p^n$ éléments.

(a) Rappeler brièvement pourquoi $L^\star$ est un groupe cyclique.

Preuve. Le groupe multiplicatif $L^\star$ est un groupe abélien fini; ainsi il existe une suite d'entiers $1 < a_1|a_2|...|a_r$ et $L^\star \simeq \frac{\mathbb{Z}}{a_1\mathbb{Z}} \times \frac{\mathbb{Z}}{a_2\mathbb{Z}} \times ... \times \frac{\mathbb{Z}}{a_r\mathbb{Z}}$. Il suit que le cardinal de $\{x \in L \mid x^{a_1} = 1\}$ est égal à a_1^r et puisque le polynôme $X^{a_1} - 1$ a au plus a_1 racines dans un corps commutatif, il suit que $a_1^r \leq a_1$; ainsi $r = 1$ et donc $L^\star \simeq \frac{\mathbb{Z}}{a_1\mathbb{Z}}$ est cyclique. ///

(b) Soit $\zeta \in L$ avec $L^\star =< \zeta >$ et $P \in \mathbb{F}_p[X]$ le générateur unitaire de $\{Q \in \mathbb{F}_p[X] \mid Q(\zeta) = 0\}$. Montrer que L est isomorphe à $\frac{\mathbb{F}_p[X]}{P\mathbb{F}_p[X]}$.

Preuve. On écrit que $P = P_1P_2$ avec $P_i \in \mathbb{F}_p[X]$, alors $P_1(\zeta)P_2(\zeta) = 0$, ainsi P_1 ou P_2 est multiple de P, d'où l'irréductibilité de P. Par la propriété universelle des anneaux de polynôme, l'application $eval_\zeta : \mathbb{F}_p[X] \to L$ telle que $eval_\zeta(Q) = Q(\zeta)$ est un homomorphisme de $\mathbb{F}_p$-algèbres. Son noyau est $P\mathbb{F}_p[X]$ et ainsi son image $\mathbb{F}_p[\zeta] \simeq \frac{\mathbb{F}_p[X]}{P\mathbb{F}_p[X]}$. On remarque que $L^\star =< \zeta >\subset \mathbb{F}_p[\zeta] \subset L$, il suit que $L = \mathbb{F}_p[\zeta]$. ///

(c) En déduire que P est un polynôme irréductible $\in \mathbb{F}_p[X]$ de degré n.

Preuve. Puisque $\frac{\mathbb{F}_p[X]}{P\mathbb{F}_p[X]}$ est un $\mathbb{F}_p$-espace vectoriel de dimension $\deg P$ il suit que $|\mathbb{F}_p[\zeta]| = p^{\deg P}$ et puisque $L = \mathbb{F}_p[\zeta]$, il suit que $n = \deg P$. ///

(3) *Unicité*

Soit L, un corps à $q = p^n$ éléments et $Q \in \mathbb{F}_p[X]$ un polynôme irréductible de degré n.

(a) Soit K contenant L un corps de rupture de $Q \in K[X]$. Soit $x \in K$ avec $Q(x) = 0$, alors $\mathbb{F}_p[x] \subset K$ est un corps de dimension n sur $\mathbb{F}_p$ et donc de cardinal $q = p^n$. Montrer que $L = \mathbb{F}_p[x]$.

Preuve. Par le théorème de Lagrange les éléments de $\mathbb{F}_p[x]$ et de L sont les racines dans K du polynôme $X^q - X$. ///

(b) En déduire que L est isomorphe à $\frac{\mathbb{F}_p[X]}{Q\mathbb{F}_p[X]}$.

Preuve. L'homomorphisme d'évaluation $eval_x : \mathbb{F}_p[X] \to \mathbb{F}_p[x]$ défini par $eval_x(R) = R(x)$ dont le noyau est $Q\mathbb{F}_p[X]$ induit un isomorphisme $\frac{\mathbb{F}_p[X]}{Q\mathbb{F}_p[X]} \simeq \mathbb{F}_p[x]$, d'où le résultat avec la question précédente. ///

(4) *Comptage des polynômes irréductibles $\in \mathbb{F}_p[X]$ de degré n.*

Soit L un corps fini à $q = p^n$ éléments.

(a) Soit $P \in \mathbb{F}_p[X]$ unitaire, irréductible de degré d. On suppose que $P|(X^q - X)$. Montrer que $d|n$.

Preuve. Puisque L est l'ensemble des racines dans L de $X^q - X$, il suit que P est un produit de polynômes de degré 1 à coefficients dans L, ainsi il existe $x \in L$ avec $P(x) = 0$. On a $\mathbb{F}_p[x] \subset L$ et donc par le théorème de la base télescopique $d = \dim_{\mathbb{F}_p} \mathbb{F}_p[x] \mid \dim_{\mathbb{F}_p} L = n$. ///

(b) Soit $P \in \mathbb{F}_p[X]$ unitaire, irréductible de degré $d|n$. Montrer que $P|(X^q - X)$.

Preuve. Soit $K \supset L$ un corps de décomposition de $P \in K[X]$ et $x \in L$ une racine de P, alors $\mathbb{F}_p[x] \simeq \frac{\mathbb{F}_p[X]}{P\mathbb{F}_p[X]}$ est un corps fini de cardinal p^d. Ainsi $x^{p^d} = x$ et donc $P|(X^{p^d} - X)$ dans $\mathbb{F}_p[X]$. Montrons que $(X^{p^d-1} - X)|(X^{p^n-1} - X)$. Il suffit de montrer que $p^d - 1 \mid p^n - 1$ ce qui est bien le cas puisque $d \mid n$. Ainsi $P|(X^{p^d} - X)|(X^{p^n} - X)$. ///

(c) Pour $d|n$, on note I_d le cardinal de l'ensemble des $P \in \mathbb{F}_p[X]$ unitaires, irréductibles de degré d avec $P|(X^q - X)$. Montrer que $p^n = \sum_{d|n} dI_d$.

Preuve. On écrit la décomposition en irréductible de $X^q - X$ dans $\mathbb{F}_p[X]$ et on en déduit une partition des racines de $X^q - X$ par leur polynôme irréductible. ///

(d) En déduire que $nI_n \leq p^n$.

Preuve. Conséquence immédiate de l'égalité précédente. ///

(e) Montrer que $nI_n \geq p^n - \sum_{1 \leq d \leq n-1} p^d$

Preuve. On a $nI_n = p^n - \sum_{d|n,\ d\neq n} dI_d \geq p^n - \sum_{d|n,\ d\neq n} p^d \geq p^n - \sum_{1\leq d\leq n-1} p^d$. ///

(f) En déduire que $nI_n \geq 2 + (p-2)\frac{p^n-1}{p-1}$.

Preuve. On a donc $nI_n \geq p^n - p\frac{p^{n-1}-1}{p-1} = 2 + (p-2)\frac{p^n-1}{p-1}$. *En particulier* $I_n \geq 1$. ///

Remarque. *Dans [F. M. 1] n°86 on trouve la formule* $\sum_{d|n} dI(d) = p^n$. *Il suit que* $I(n) = \frac{1}{n}\sum_{d|n}\mu(\frac{n}{d})p^d$, *où* $\mu(.)$ *est la fonction de Möbius.*

Exercice 4 Racines d'un polynôme irréductible dans $\mathbb{F}_p[X]$ et signature de l'automorphisme de Frobenius, [F. M. 1] n°72 par.5 p.180.

Soit $P \in \mathbb{F}_p[X]$ un polynôme irréductible. Soit $z \in \Omega$ une racine de P dans une clôture algébrique Ω. Soit φ le $\mathbb{F}_p$-automorphisme de Ω défini par $\varphi(x) = x^p$.

(1) Montrer que z est une racine simple de P.

Preuve. Sinon $P'(z) = 0$ *ainsi* z *est racine du polynôme* $P' \in \mathbb{F}_p[X]$ *qui est nul ou de degré* $< d = \deg P$; *puisque* P *est irréductible,* P *est le générateur de l'idéal des polynômes de* $\mathbb{F}_p[X]$ *qui s'annulent en* z; *ainsi la seule possibilité est que* $P' = 0$ *i.e.* $P \in \mathbb{F}_p[X^p]$ *et puisque si* $a \in \mathbb{F}_p$ *on* $a = a^p$, *il suit que* $P = Q^p$ *avec* $Q \in \mathbb{F}_p[X]$, *ce qui est une contradiction.*

(2) Montrer que $\varphi(z) = z^p$ est une racine de P.

Preuve. On écrit $P = \sum_i a_i X^i$, *alors* $P(z^p) = \sum_i a_i z^{pi} = (\sum_i a_i z^i)^p$ *puisque* $a_i^p = a_i$.///

(3) Soit d le degré de P. Quel est le corps $\mathbb{F}_p[z]$? Montrer que $\varphi^d(z) = z$.

Preuve. Le corps $\mathbb{F}_p[z]$ *est isomorphe au corps* $\frac{\mathbb{F}_p[X]}{(P)}$; *c'est en particulier un espace vectoriel de dimension* $d = \deg P$ *(faire la division euclidienne par* P*); il est donc de cardinal* p^d *et donc isomorphe au corps fini* $\mathbb{F}_{p^d}$, *il suit du théorème de Lagrange que* $\varphi^d(z) = z$.

(4) Soit $n > 1$ avec $\varphi^n(z) = z$, montrer que d divise n. En déduire la liste des racines de P.

Preuve. On écrit $n = sd + r$ *avec* $0 \leq r < d$. *Puisque* $\varphi^d(z) = z$, *il suit que* $\varphi^r(z) = z$; *ainsi si* $r \neq 0$, $z \in \mathbb{F}_{p^r}$ *et donc* $\mathbb{F}_p[z] \subset \mathbb{F}_{p^r}$ *en particulier* $p^d \leq p^r$ *ce qui est absurde. Montrons que* $\varphi^i(z) \neq \varphi^j(z)$ *pour* $0 \leq i < j < d$. *En effet sinon* $\varphi^{j-i}(z) = z$ *et donc* $d|j-i$. *Ainsi les* d *éléments* $\varphi^i(z)$, $0 \leq i < d$ *sont les* d *racines de* P.

(5) Soit $\mathbb{F}_q$ le corps à $q = p^s$ éléments. L'application φ induit un automorphisme de $\mathbb{F}_q$ et donc une permutation des q éléments de $\mathbb{F}_q$. Montrer que les ordres des cycles qui apparaissent dans cette décomposition divisent s.

Preuve. Soit $z \in \mathbb{F}_q$, *l'orbite de* z *sous* $< \varphi >$ *est d'ordre* d *où* $d = [\mathbb{F}_p[z] : \mathbb{F}_p]$ *et puisque* $\mathbb{F}_p \subset \mathbb{F}_p[z] \subset \mathbb{F}_q$, $d|s$.

(6) Déduire de ce qui précède la décomposition de φ en produit de cycles à supports disjoints.

Preuve. L'orbite de $z \in \mathbb{F}_q$ *sous* $< \varphi >$ *est* $(z, .., \varphi^i(z), .., \varphi^{d-1}(z))$ *et* $P(X) := \prod_{0\leq i<d}(X - \varphi^i(z))$ *est polynôme irréductible de* z *sur* $\mathbb{F}_p$. *Ainsi* $\varphi = \prod_{d|s}\prod_{P\in\mathcal{P},\ \deg P=d,\ P(z)=0}(z, .., \varphi^i(z), .., \varphi^{d-1}(z))$ *où* $\mathcal{P}$ *désigne l'ensemble des polynômes irréductibles unitaires de* $\mathbb{F}_p[X]$. *En particulier si* I_d *est le nombre de polynômes irréductibles unitaires de* $\mathbb{F}_p[X]$ *de degré* d *la signature de la permutation induite par* φ *est* $(-1)^{\sum_{d|s}(d-1)I_d}$. *En particulier si* s *est impair alors* $d-1$ *est pair pour* $d|s$ *et donc la signature vaut* 1.

Exercice 5 Comptage des polynômes irréductibles sur $\mathbb{F}_p$ avec la formule de Burnside sur le nombre d'orbites dans une action de groupes ([F. M. 1] n°59 p. 148).

Soit $n > 0$ et $q = p^n$, on note F l'automorphisme de $\mathbb{F}_q$ avec $F(x) = x^p$. Le groupe $< F >$ est cyclique d'ordre n et agit sur $\mathbb{F}_q$ par $F(x) = x^p$. Montrer que l'orbite de x coïncide avec l'ensemble des racines du polynôme irréductible de x sur $\mathbb{F}_p$ et en déduire la formule $\sum_{d|n} I(d) = \frac{1}{n}\sum_{1\leq i\leq n} p^{(i,n)} = \frac{1}{n}\sum_{d|n}\varphi(\frac{n}{d})p^d$ où $I(d)$ est le nombre de polynômes unitaires de degré d irréductibles de $\mathbb{F}_p[X]$. En déduire que si ℓ est premier alors $I(\ell) = \frac{p^\ell - p}{\ell}$.

Remarque. Dans [F. M. 1] n°86 on trouve la formule $\sum_{d|n} dI(d) = p^n$ *(on répartit les éléments de* F_{p^n} *par leur polynôme irréductible) il suit que* $I(n) = \frac{1}{n}\sum_{d|n}\mu(\frac{n}{d})p^d$, *où* $\mu(.)$ *est la fonction de Möbius.*

On en déduit facilement que $I(n) > 0$. Il est plus habile comme vu dans l'exercice 3 de remarquer que $nI_n = p^n - \sum_{d|n,\ d\neq n} dI_d \geq p^n - \sum_{d|n,\ d\neq n} p^d \geq p^n - \sum_{1\leq d\leq n-1} p^d \geq p^n - p\frac{p^{n-1}-1}{p-1} = 2 + (p-2)\frac{p^n-1}{p-1} > 0$.

Exercice 6 Calcul du symbole quadratique $(\frac{2}{p})$, [Se.] p. 16.

Soit $p > 2$ un nombre premier et $\mathbb{F}_p$ le corps fini à p éléments et L un corps de décomposition du polynôme $X^8 - 1 \in \mathbb{F}_p[X]$.

(1) Soit $U_8 := \{x \in L,\ |\ x^8 = 1\}$. Justifier que U_8 est un sous-groupe cyclique d'ordre 8 de $L^\times$.
Preuve. Puisque L est un corps commutatif $|U_8| \leq \deg(X^8 - 1)$ et puisque $p > 2$, il suit que $PGCD(X^8-1, 8X^7) = 1$; ainsi $|U_8| = 8$. Ainsi U_8 est un sous-groupe fini d'un corps commutatif; il est donc cyclique. Pus simplement on peut factoriser $X^8-1 = (X^4-1)(X^4+1)$ et ainsi partitionner les racines de $X^8 - 1$ en $\{x \in L,\ |\ x^4 = 1\} \cup \{x \in L,\ |\ x^4 = -1\}$ et puisque chaque partie est de cardinal ≤ 4, il suit que $|\{x \in L,\ |\ x^4 = -1\}| = 4$; on a ainsi exhibé 4 racines primitives 8-ième de l'unité. ///

(2) Soit $\alpha \in L$, une racine primitive 8-ième de l'unité. Soit $y := \alpha + \alpha^{-1}$. Montrez que $y^2 = 2$.
Preuve. On développe $y^2 = \alpha^2 + 2 + \alpha^{-2} = 2$ puisque $\alpha^4 + 1 = 0$. ///

(3) On suppose que $p = \pm 1$ modulo 8. Montrer que $y \in \mathbb{F}_p$.
Preuve. On calcule $y^p = \alpha^p + \alpha^{-p}$ et pour $p = \pm 1$ modulo 8 on retrouve y. Ainsi $y \in \mathbb{F}_p$. ///

(4) On suppose que $p = \pm 5$ modulo 8. Montrer que $y \notin \mathbb{F}_p$.
Preuve. On calcule $y^p = \alpha^p + \alpha^{-p}$ et pour $p = \pm 5$ modulo 8 on trouve $-y$. Ainsi $y \notin \mathbb{F}_p$. ///

(5) En déduire que 2 est un carré modulo p si et seulement si $p = \pm 1$ modulo 8.
Preuve. Puisque $y^2 = 2$ il suit que 2 est un carré modulo p si et seulement si $y \in \mathbb{F}_p$. Puisque p est impair il suit que $p = \pm 1$ ou $p = \pm 5$ modulo 8. Le résultat suit alors des questions précédentes. ///

Exercice 7 Il y a une infinité de nombres premiers congrus à 7 mod 8 en utilisant le symbole quadratique $(\frac{2}{p})$.

On rappelle, [Se.] p. 15 que $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.

On suppose qu'il n'y a qu'un nombre fini de nombres premiers congrus à 7 mod 8. Soit donc $\{p_1, p_2, ..., p_n\}$ l'ensemble des nombres premiers congrus à 7 modulo 8.

(1) Soit $p \neq 2$ un diviseur premier de $N := (4p_1...p_n)^2 - 2$. Montrer que $p = \pm 1$ mod 8.
Preuve. On remarque que $2 = (4p_1...p_n)^2$ mod 8 ainsi par la question précédente $p = \pm 1$ mod 8. ///

(2) En déduire qu'il existe un diviseur premier q de N qui est congru à -1 modulo 8. Conclure.
Preuve. On a $\frac{N}{2} = 8(p_1...p_n)^2 - 1$, ainsi il existe un diviseur premier q de N qui est congru à -1 modulo 8 mais $q \notin \{p_1, p_2, ..., p_n\}$ ce qui donne une contradiction. ///

Exercice 8 Loi de réciprocité quadratique via les polynômes cyclotomiques, [F. M. 2] p. 243.

Exercice 9 Sur les sous-groupes cycliques de $Gl_n(\mathbb{F}_q)$ d'ordre $q^n - 1$, [F. M. 2] p. 53.

Exercice 10 Signature d'un automorphisme d'un espace vectoriel sur un corps fini. Application à la signature de l'automorphisme de Frobenius de $\mathbb{F}_q$. [F. M. 1] n° 72 partie 4 p. 175

Exercice 11 Sous-groupes de $GL_n(\mathbb{Z})$ qui sont de torsion, [F. M. 1] n°26 p. 46.

Exercice 12 Classification des coniques sur un corps fini, [F. M. 1] n°129 p. 373, [Fr. MMG] p. 323.

Classification des quadriques affines, [Fr. MMG] p. 300.
Points rationnels sur une conique sur un corps fini, [F. M. 1] $n°131$ question 6 p. 377.
Soit $p > 2$ un nombre premier et $q := p^n$. On note $F(X,Y) := X^2 + Y^2 + 1 \in \mathbb{F}_q[X,Y]$.

(1) (a) Montrer que -1 est un carré dans $\mathbb{F}_q$ ssi $q = 1 \mod 4$.
    (b) Déterminer les couples (p,n) pour lesquels $q = 1 \mod 4$.
(2) Montrer que $\{1 + \mathbb{F}_q^2\} \cap \{-\mathbb{F}_q^2\} \neq \emptyset$. En déduire qu'il existe $(x_0, y_0) \in \mathbb{F}_q \times \mathbb{F}_q$ avec $F(x_0, y_0) = 0$.
(3) On suppose que $q \neq 1 \mod 4$, montrer que $y_0 \neq 0$ et en posant $X = x_0 + X'$ et $Y = y_0 + Y'$ montrer que le nombre de solutions dans $\mathbb{F}_q \times \mathbb{F}_q$ de $F(x,y) = 0$ vaut $q + 1$.
(4) On suppose que $q = 1 \mod 4$, montrer que l'on peut prendre $y_0 = 0$ et en posant $X = x_0 + X'$ et $Y = y_0 + Y'$ montrer que le nombre de solutions dans $\mathbb{F}_q \times \mathbb{F}_q$ de $F(x,y) = 0$ vaut $q - 1$.

Exercice 13 Il n'existe pas d'anneaux A dont le groupe des inversibles $A^\times$ est d'ordre 5, [F. M. 1] $n°107$ p. 296.

On suppose que A est un anneau unitaire dont le groupe des inversibles $A^\times$ est d'ordre 5.

(1) Montrer que $1 = -1$ dans A. En déduire que A contient un sous-corps isomorphe à $\mathbb{F}_2$ (on le notera encore $\mathbb{F}_2$).

    Preuve. On remarque que $(-1)^2 = 1$, ainsi $-1 \in A^\times$ et son ordre est 1 ou 2. Par le théorème de Lagrange il n'est pas 2 c'est donc que $1 = -1$ dans A. Ainsi $2.1_A = 0$ et donc l'homomorphisme canonique $\mathbb{Z} \to A$ qui envoie $1 \in \mathbb{Z}$ sur 1_A est de noyau $\subset 2\mathbb{Z}$ et puisque cet homomorphisme n'est pas l'homomorphisme nul le noyau est égal à $2\mathbb{Z}$. Il suit du théorème de factorisation que $\mathbb{F}_2$ s'injecte dans A et son image $\{0, 1_A\}$ est un sous-corps de A isomorphe à $\mathbb{F}_2$. ///
(2) Soit B le sous-anneau de A engendré par $A^\times$, montrer que $A^\times = B^\times$.

    Preuve. Par construction $B \subset A$ et donc $B^\times \subset A^\times$ et puisque $A^\times \subset B$ on a l'égalité $A^\times = B^\times$. ///
(3) Soit ζ un générateur de $A^\times$, justifier l'existence d'un homomorphisme de $\mathbb{F}_2$-algèbre $\rho : \mathbb{F}_2[X] \to A$ vérifiant $\rho(P(X)) = P(\zeta)$.

    Preuve. C'est la propriété universelle des anneaux de polynômes. ///
(4) Montrer que $B = \operatorname{Im}\rho$ et que $\ker\rho = S(X)\mathbb{F}_2[X]$ avec $S(X)$ unitaire divisant $X^5 - 1$.

    Preuve. Par construction $\operatorname{Im}\rho = \mathbb{F}_2[\zeta]$ et c'est le plus petit sous-anneau de A contenant ζ et donc $A^\times$; c'est donc B. Le noyau est un idéal monogène ($\mathbb{F}_2[X]$ est un anneau principal) non nul et puisque $\rho(X^5 - 1) = 0$, le résultat suit. ///
(5) Montrer que $\frac{X^5-1}{X-1}$ est irréductible sur $\mathbb{F}_2$. En déduire la liste des diviseurs de $X^5 - 1$ dans $\mathbb{F}_2[X]$.

    Preuve. On a $X^5 - 1 = (X-1)(X^4 + X^3 + X^2 + X + 1)$. Le polynôme $X^4 + X^3 + X^2 + X + 1$ n'a pas de racine dans $\mathbb{F}_2$ et il n'est pas égal à $(X^2 + X + 1)^2 = X^4 + X^2 + 1$ et puisque $X^2 + X + 1$ est le seul irréductible de degré 2 dans $\mathbb{F}_2[X]$, il suit que $X^4 + X^3 + X^2 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$. Ainsi $\{1, X - 1, X^4 + X^3 + X^2 + X + 1, X^5 - 1$ sont les diviseurs de $X^5 - 1$ dans $\mathbb{F}_2[X]$. ///
(6) En remarquant que $B \simeq \frac{\mathbb{F}_2[X]}{S(X)\mathbb{F}_2[X]}$, conclure à une contradiction.

    Preuve. Puisque $S(X) \neq 1$ il suit que l'anneau B est soit isomorphe à $B_1 := \frac{\mathbb{F}_2[X]}{(X-1)} = \mathbb{F}_2$, soit isomorphe à $B_2 := \frac{\mathbb{F}_2[X]}{(X^4+X^3+X^2+X+1)} \simeq \mathbb{F}_{2^4}$ ou soit isomorphe à $B_3 := \frac{\mathbb{F}_2[X]}{(X^5-1)} \simeq B_1 \times B_2$ par le théorème des restes chinois. On a dans tous les cas une contradiction avec $|B^\times| = 5$. ///

Exercice 14 Matrices de Hadamard et carrés dans $\mathbb{F}_q^\times$, [F. M. 2] p. 115 question 4.

Exercice 15 On peut évoquer le logarithme discret pour l'échange de clés voir
Échange de clés Diffie-Hellman — Wikipédia