EPFL Automne 2022
Algebre Lineaire Avancee, MATH-110

Corrigé - Série 7

Tous les exercices seront corrigés. La correction sera postée sur le moodle après 2 semaines.

Vous êtes fortement encouragés à essayer de résoudre (eventuellement à plusieurs) l'exercice ($\star$) et à rendre votre solution (eventuellement à plusieurs) avant le dimanche de la semaine suivant celle où la sèrie a été postée. Il faudra transmettre votre solution sur moodle, sous forme de fichier pdf (eventuellement tapé en LaTeX) en suivant le lien à cet effet dans la semaine de la série.

1 Question de dimension

Exercice 1. Soient X et Y des EVs sur un corps K. On note leurs produit

$$X \times Y = \{(x, y), x \in X, y \in Y\}$$

On rappelle que $X \times Y$ a une structure d'espace vectoriel en posant (avec less additions et multiplications par les scalaires convenables)

$$(x, y) + (x', y') = (x + x', y + y'), k.(x, y) = (k.x, k.y)$$

Pour $\mathcal{F}_X \subset X$, $\mathcal{F}_Y \subset Y$ des sous-enesmbles de X et Y, on note

$$\mathcal{F}_X \oplus \mathcal{F}_Y = \{(x, 0_Y), x \in \mathcal{F}_X\} \cup \{(0_X, y), y \in \mathcal{F}_Y\}$$

On suppose que X et Y sont de dimension finie.

1. Montrer que si $\mathcal{F}_X$ et $\mathcal{F}_Y$ sont des familles libes alors $\mathcal{F}_X \oplus \mathcal{F}_Y$ est libe.
2. Montrer que si $\mathcal{F}_X$ et $\mathcal{F}_Y$ sont generatrices alors $\mathcal{F}_X \oplus \mathcal{F}_Y$ est generatrice.
3. Montrer que $X \times Y$ est de dimension finie et que

$$\dim(X \times Y) = \dim X + \dim Y$$

Solution 1. 1. Notons tout d'abord que comme X et Y sont supposé de dimension finie, $\mathcal{F}_X$ et $\mathcal{F}_Y$ doivent être de cardinalité finie (car ce sont des familles libres). Ainsi on peut écrire $\mathcal{F}_X = \{e_1, ..., e_r\}$, $\mathcal{F}_Y = \{f_1, ..., f_s\}$ pour $r, s \in \mathbb{N}$ et $e_i \in X$ $\forall i \leqslant r$, $f_j \in Y$ $\forall j \leqslant s$. Supposons qu'il existe des coefficients $\lambda_i \in K$ $\forall i \leqslant r$ et $\mu_j \in K$ $\forall j \leqslant s$ tels que

$$\sum_{i \leqslant r} \lambda_i (e_i, 0_Y) + \sum_{j \leqslant s} \mu_j (0_X, f_j) = (0_X, 0_Y)$$

Ainsi on obtient que

$$\left(\sum_{i \leqslant r} \lambda_i e_i, \sum_{j \leqslant s} \mu_j f_j \right) = (0_X, 0_Y)$$

et donc

$$\sum_{i \leqslant r} \lambda_i e_i = 0_X, \ \sum_{j \leqslant s} \mu_j f_j = 0_Y$$

Ainsi comme $\mathcal{F}_X$ et $\mathcal{F}_Y$ sont libres, on obtient que $\lambda_i = 0_K$ $\forall i \leqslant r$ et $\mu_j = 0_K$ $\forall j \leqslant s$. On en déduit que $\mathcal{F}_X \oplus \mathcal{F}_Y$ est une famille libre comme voulu $\square$

2. Soit $(x, y) \in X \times Y$. Comme $\mathcal{F}_X$ est géneratrice de X, il existe une sous famille finie $S_X \subset \mathcal{F}_X$ et des coefficients $\lambda_u \in K$ $\forall u \in S_X$ tels que $x = \sum_{u \in S_X} \lambda_u u$. Similairement, il existe une sous famille finie $S_Y \subset \mathcal{F}_Y$ et des coefficients $\lambda_v \in K$ $\forall v \in S_Y$ tels que $y = \sum_{v \in S_Y} \lambda_v v$. Ainsi on obtient que

$$(x, y) = \sum_{u \in S_X} \lambda_u (u, 0_Y) + \sum_{v \in S_Y} \lambda_v (0_X, v)$$

Comme $(u, 0_Y), (0_X, v) \in \mathcal{F}_X \oplus \mathcal{F}_Y$ $\forall u \in S_X, v \in S_Y$, on en déduit que $\mathcal{F}_X \oplus \mathcal{F}_Y$ est géneratrice de $X \times Y$ $\square$

3. Soit $\mathcal{B}_X \subset X$ et $\mathcal{B}_Y \subset Y$ des bases de X et Y respectivements. Alors par les deux questions précedentes, $\mathcal{B}_X \oplus \mathcal{B}_Y$ est une famille libre et géneratrice de $X \times Y$, et donc une base. Finalement, on a

$$\dim(X \times Y) = |\mathcal{B}_X \oplus \mathcal{B}_Y| = |\mathcal{B}_X| + |\mathcal{B}_Y| = \dim X + \dim Y$$

comme voulu $\square$

Remarque 1.1. À noter que la supposition que X et Y sont de dimensions finie n'est pas nécessaire pour la partie 1 et 2 : il faudrait cependant modifier l'argument de la question 1 pour regarder des combinaisons linéaires sur des sous-ensembles finis arbitraire de $\mathcal{F}_X \oplus \mathcal{F}_Y$.

Exercice 2. 1. Soit K un corps et $k \subset K$ un sous-corps. Montrer que K est un k-espace vectoriel.

2. Soit K un corps fini de caracteristique $p > 0$ et

$$\mathbb{F}_p = \mathrm{Can}_K(\mathbb{Z}) = \mathbb{Z}.1_K \subset K$$

le sous-corps premier. Montrer que K est de dimension finie ($d \geqslant 1$) sur $\mathbb{F}_p$ et que $|K| = p^d$.

3. On suppose que K est encore contenu dans un autre corps fini L. Ainsi

$$\mathbb{F}_p \subset K \subset L$$

et on a donc (par la question precedente) $|L| = p^{d'}$ avec $d' \geqslant 1$. Montrer que d divide d' (on montrera que le quotient d'/d est une certaine dimension).

Solution 2. 1. Puisque K est un corps, en particulier $(K, +)$ est un groupe abélien. La loi de multiplication de K

$$\begin{array}{ccc} K \times K & \mapsto & K \\ (x, y) & \mapsto & xy \end{array}$$

restreint a k :

$$\begin{array}{ccc} K \times k & \mapsto & K \\ (x, y) & \mapsto & xy \end{array}$$

munit K d'une structure de k-espace vectoriel. L'associativité et la distributivité de cette loi suivent directement des propriétés de K $\square$

2. Comme K est fini, K a une famille génératrice finie (par exemple tout K). Ainsi, K vu comme $\mathbb{F}_p$-espace vectoriel est de dimension finie que nous noterons d. Par le cours, nous savons que $K \cong \mathbb{F}_p^d$. En particulier, $|K| = |\mathbb{F}_p^d| = p^d$ $\square$

3. Pusique $\mathbb{F}_p \subset K \subset L$, L peut être vu comme un $\mathbb{F}_p$-espace vectoriel ou comme un K-espace vectoriel. Posons $d' = \dim_{\mathbb{F}_p} L$ et $d" = \dim_K L$. Par la question précedente, $|L| = |\mathbb{F}_p^{d'}| = p^{d'} = |K|^{d"} = (p^d)^{d"} = p^{dd"}$. Nous avons donc que $d' = dd"$ ce qui est équivalent a dire que d divise d' $\square$

Remarque 1.2. Cet exercice se géneralise à la notion d'extension de corps : étant donné un corps K, on appel extension de corps un morphisme injéctif $\phi : K \hookrightarrow L$ dans un autre corps L (ce qui équivaut à dire que K est un sous-corps de L). Alors si L est de dimension finie sur $\phi(K)$ avec la structure d'espace vectoriel que l'ont vient de voir, on dit que cette extension est de degré finie et on note le degré $[L : K]$. Alors on vient de montrer que pour une chaine d'extensions de degré finie $K \subset L \subset F$, on a $[F : K] = [F : L][L : K]$. Ceci est plus qu'un exercice en cardinalité, car le degré a une signification plus profonde reliée aux équations polynomiales qui admettent des solutions sur L et non sur K. Ce concept est approfondi dans le cours d'Anneaux et Corps de BA4.

2 Autour du Thm Noyau-Image

Exercice 3. Soit K un corps. Soit $\varphi : K^2 \to K^2$ l'application linéaire définie par

$$\varphi : \begin{array}{ccc} K^2 & \mapsto & K^2 \\ (x,y) & \mapsto & (2x+y, x+2y) \end{array}$$

(ici on notera $2, 3, ...$ pour $2_K = 2.1_K,\ 3_K = 3.1_K,\ ...$)

Montrer avec un minimum de calculs que $\ker(\varphi) = \{0_2\}$ et $\mathrm{Im}(\varphi) = K^2$.

Solution 3. On va montrer que $\mathrm{Im}(\varphi) = K^2$ en montrant que $\{(1,0),(0,1)\} \subset \mathrm{Im}(\varphi)$, car c'est une base de K^2. Il suffit de deviner les valeurs de x et y à prendre pour obtenir ces vecteurs. Par inspection on voit que quand $\mathrm{car}(K) \neq 2$, on a $\varphi(1,-1) = (1,0)$ et $\varphi(-1,2) = (0,1)$. Ainsi dans ce cas $\mathrm{Im}(\varphi) = K^2$ pour $\mathrm{car}(K) \neq 2$. Dans le cas ou $\mathrm{car}(K) = 2$, on a $\varphi(x,y) = (y, x+y)$. Ainsi on a $\varphi(1,1) = (1,0)$ et $\varphi(0,1) = (0,1)$, et donc $\mathrm{Im}(\varphi) = K^2$.

Ainsi quoi qu'il arrive, $\mathrm{Im}(\varphi) = K^2$, et donc par le théorème noyau image,

$$\dim(\ker(\varphi)) + 2 = 2 \implies \dim(\ker(\varphi)) = 0$$

et donc $\ker(\varphi) = \{0_2\}$ comme voulu □

Exercice 4. Soit $\varphi : K^2 \to K^2$ l'application linéaire définie par

$$\varphi : \begin{array}{ccc} K^2 & \mapsto & K^2 \\ (x,y) & \mapsto & (3x+3y, x+4y) \end{array}$$

(ici on notera $2, 3, ...$ pour $2_K = 2.1_K,\ 3_K = 3.1_K,\ ...$)

1. Trouver avec un minimum de calculs les dimensions de $\ker(\varphi)$ et $\mathrm{Im}(\varphi)$ (en fonction de la caractéristique de K).
2. Donner (encore avec le minimum de calculs) une base du noyau et de l'image de φ.

Solution 4. 1. On va séparer entre $\mathrm{car}(K) = 2, 3$ ou autre (la motivation pour ces choix vient des coefficients devant x et y dans l'expression de φ).

Supposons d'abord que $\mathrm{car}(K) = 2$. Alors $\varphi(x,y) = (x+y, x)$. On voit donc que $\ker(\varphi) = \{0_2\}$, et ainsi par le théorème noyau-image $\dim \mathrm{Im}(\varphi) = 2$.

Supposons maintenant que $\mathrm{car}(K) = 3$. Alors $\varphi(x,y) = (0, x+y)$. On voit donc que $\varphi(1,-1) = (0,0)$, et que $\varphi(0,1) = (0,1) \neq (0,0)$ donc $\dim \ker(\varphi) = 1$ et $\dim \mathrm{Im}(\varphi) = 1$ encore par le théorème noyau-image.

Finalement, supposons que $\mathrm{car}(K) \neq 2, 3$. Alors $\varphi(1,-1) = (0,-3)$ et $\varphi(1,0) = (3,1)$ et comme $(0,-3), (3,1)$ sont linéairement indépendants et non nuls on obtient que $\dim \mathrm{Im}(\varphi) = 2$ et $\dim \ker(\varphi) = 0$ □

2. Comme on travail en petites dimensions, les bases sont simples à trouver.
   Tout d'abord pour $\text{car}(K) = 2$, par la partie précedente on obtient aucune base de $\ker(\varphi)$ et la base $\{(1,0),(0,1)\}$ de $\text{Im}(\varphi) = K^2$.
   Ensuite pour $\text{car}(K) = 3$ par la partie précedente il suffit de trouver un élement non nul de $\ker(\varphi)$ et de $\text{Im}(\varphi)$. Ainsi une base de $\ker(\varphi)$ est $\{(1,-1)\}$ et une base de $\text{Im}(\varphi)$ est $\{(0,1)\}$.
   Finalement pour $\text{car}(K) \neq 2,3$, on à un cas similaire au cas $\text{car}(K) = 2$: $\text{Im}(\varphi) = K^2$ donc une base de $\text{Im}(\varphi)$ est donnée par $\{(1,0),(0,1)\}$ et $\ker(\varphi)$ n'admet pas de base.

Exercice 5. Soit K un corps de caracteristique 0, $V = K^5$ et

$$W = \{(a,b,c,d,e) \in V,\ a+b = c+d,\ a+2c = 0, 2c+b+4d = 0\}.$$

1. Montrer que W est un SEV de K^5 en montrant que W est le noyau d'une application linéaire convenable.
2. Calculer $\dim W$ (éventuellement en utilisant le Thm Noyau-Image).
3. Donner une base de W

Solution 5. 1. On peut réecrire les éléments $(a,b,c,d,e) \in W$ comme les éléments de K^5 satisfaisant le système suivant :

$$\begin{cases} a+b-c-d = 0 \\ a+2c = 0 \\ 2c+b+4d = 0 \end{cases}$$

Ainsi en considérant l'application

$$\varphi : \begin{array}{ccc} K^5 & \mapsto & K^3 \\ (a,b,c,d,e) & \mapsto & (a+b-c-d, a+2c, 2c+b+4d) \end{array}$$

on voit que $W = \varphi^{-1}(0_3)$. Il suffit de montrer que φ est une application linéaire, ce qui est facilement vérifiable de sa définition. Ainsi $W = \ker(\varphi)$ et donc W est un sous-espace vectoriel de K^5

2. On prétend que $\dim \text{Im}(\varphi) = 3$. Pour montrer ceci il suffit de montrer que $(0,1,0) \in \text{Im}(\varphi)$ et que $\langle (1,0,0),(0,0,1)\rangle \subset \text{Im}(\varphi)$. Il est facile d'obtenir deux vecturs linéairement indépendants de $\langle (1,0,0),(0,0,1)\rangle$: en prenant $a = c = 0$ on s'assure que la deuxiême coordonée est nulle. Alors $\varphi(0,1,0,0,0) = (1,0,1)$ et $\varphi(0,1,0,1,0) = (0,0,5)$ qui sont les deux vecteurs indépendants recherchés. Il reste à trouver une préimage de $(0,1,0)$. En prenant $a = 1, c = 0$ on obtient 1 dans la deuxiême coordonée. On veut alors trouver une solution de

$$\begin{cases} b-d = -1 \\ b+4d = 0 \end{cases}$$

On obtient $5d = 1 \implies d = \frac{1}{5}$ et $b = -\frac{4}{5}$. Ainsi $\varphi(1, -\frac{4}{5}, 0, \frac{1}{5}, 0)$. Ainsi on a bien que $\dim \mathrm{Im}(\varphi) = 3 \implies \dim W = 2$ par le théorème noyau-image.

Remarque 2.1. Ceci n'est pas une approche sytématique de ce type de problème, mais quand on a peu de variables et un système à coefficients pas trop compliqués, c'est toujours une bonne idée de d'abord essayer de résoudre par inspection avant d'appliquer une méthode systèmatique de résolution de système : ceci peut faire gagner du temps. On présente une approche plus systèmatique de la prochaine partie, mais essayez de le résoudre aussi d'abord par inspection. Vous verrez ainsi les avantages et inconvénients des deux méthodes.

3. Analysons plus en détails le système donné définissant W.

$$\begin{cases} a+b-c-d=0 \\ a+2c=0 \\ 2c+b+4d=0 \end{cases} \iff \begin{cases} -2c+b-c-d=0 \\ a=-2c \\ 2c+b+4d=0 \end{cases} \iff \begin{cases} b=3c+d \\ a=-2c \\ 2c+3c+d+4d=0 \end{cases}$$

$$\iff \begin{cases} b=3c+d \\ a=-2c \\ 5(c+d)=0 \end{cases}$$

$$\iff \begin{cases} b=2c \\ a=-2c \\ d=-c \end{cases}$$

Ainsi $W = \{c(-2,2,1,-1,0) + e(0,0,0,0,1) : c, e \in K\}$. Une base de W est donc donnée par $\{(-2,2,1,-1,0), (0,0,0,0,1)\}$. (On vient de montrer que cette famille est génératrice, et comme $\dim W = 2$ elle doit être libre).

Exercice 6. ($\star$) Soient $X, Y \subset V$ des SEV d'un EV de dimension finie et $X+Y \subset V$ leur somme (qui est un SEV de V). On rappelle que X et Y sont en somme directe si $X \cap Y = \{0_V\}$ et on ecrit cela $X \oplus Y$.

1. Montrer que $\dim X + \dim Y = \dim(X+Y) + \dim(X \cap Y)$.
2. On suppose que $\dim X + \dim Y = \dim V$. Montrer que les propriétés suivantes sont équivalentes :
   (a) $X \cap Y = \{0_V\}$
   (b) $X + Y = V$
   (c) $X \oplus Y = V$

Pour résoudre ce probleme, on pourra appliquer le Thm Noyau-Image à l'application linéaire

$$\bullet + \bullet : \begin{array}{ccc} X \times Y & \mapsto & V \\ (x,y) & \mapsto & x+y \end{array}.$$

Solution 6. 1. En appliquant le théorème Noyau-Image à l'application linéaire $\bullet + \bullet$, nous avons que

$$\dim X \times Y = \dim \mathrm{Im}(\bullet + \bullet) + \dim \ker(\bullet + \bullet)$$

Remarquons pour commencer que $\dim X \times Y = \dim X + \dim Y$ par l'exercice 1.

Maintenant, observons que :

$$\begin{aligned} \mathrm{Im}(\bullet + \bullet) &= \{x + y : \exists\ (x, y) \in X \times Y\ t.q\ \ \bullet + \bullet\ ((x, y)) = x + y\} \\ &= X + Y \end{aligned}$$

donc $\dim \mathrm{Im}(\bullet + \bullet) = \dim(X + Y)$. De plus observons que

$$\begin{aligned} \ker(\bullet + \bullet) &= \{(x, y) \in X \times Y : x + y = 0\} \\ &= \{(x, -x) : x \in X, -x \in Y\} \\ &= \{(x, -x) : x \in X \cap Y\} \end{aligned}$$

Remarquer que $\ker(\bullet + \bullet)$ est isomorphe à $X \cap Y$. En effet, l'application

$$\phi : \begin{array}{ccc} \ker(\bullet + \bullet) & \mapsto & X \cap Y \\ (x, -x) & \mapsto & x \end{array}$$

est linéaire et bijective.

Linéarite : $\forall a \in K, (x, -x), (y, -y) \in \ker(\bullet + \bullet)$,

$$\begin{aligned} \phi(a(x, -x) + (y, -y)) &= \phi((ax + y, -ax - y)) \\ &= ax + y \\ &= a\phi((x, -x)) + \phi((y, -y)) \end{aligned}$$

Injectivité : $\ker \phi = \{(x, -x) \in \ker(\bullet + \bullet) : \phi((x, -x)) = x = 0\} = \{(0, 0)\}$

Surjectivité : soit $x \in X \cap Y$ arbitraire, alors $x = \phi((x, -x))$, donc ϕ est surjective.

Ainsi $\ker(\bullet + \bullet) \cong X \cap Y$ et en particulier $\dim \ker(\bullet + \bullet) = \dim X \cap Y$.

Finalement, ceci nous permet d'écrire

$$\dim X + \dim Y = \dim(X + Y) + \dim(X \cap Y)$$

□

2. Nous alons montrer la chaine d'implications $(a) \implies (b) \implies (c) \implies (a)$.

$(a) \implies (b)$: Comme $X \cap Y = \{0_V\}$, on a $\dim X + \dim Y = \dim(X + Y)$ par la partie précédente. Ainsi par l'hypothèse $\dim X + \dim Y = \dim V$ on obtain $\dim V = \dim(X + Y)$ et donc $X + Y = V$ car $X + Y$ est un SEV de V.

$(b) \implies (c)$: Comme $X+Y=V$ on a $\dim(X+Y)=\dim(V)=\dim X+\dim Y$. Ainsi par la partie précédente, $\dim X\cap Y=0$, et donc X et Y sont en somme directe.

$(c) \implies (a)$: Ceci suit directement de la définition d'être en somme directe : écrire $X\oplus Y$ pour des SEV de V implique que $X\cap Y=\{0_V\}$.

Ceci démontre les équivalences voulues $\square$

3 Espace vectoriel quotient

Exercice 7. Soit V un K-EV et $U\subset V$ un SEV. On va défini la notion d'espace vectoriel quotient V/U. La relation sur $(v,v')\in V\times V$ donnée par

$$v\sim_U v' \iff v-v'\in U$$

est une relation d'équivalence dont l'ensemble des classes d'équivalences est donné par le sous-ensemble de $\mathscr{P}(V)$

$$V/U=\{v(\text{mod } U):=v+U : v\in V\}$$

On muni alors l'espace quotient V/U d'une structure de groupe (commutatif) en posant

$$v(\text{mod } U)+_{V/U} v'(\text{mod } U)=(v+U)+(v'+U)=v+v'(\text{mod } U)$$

on peut vérifier (comme pour le cas du quotient d'un anneau commutatif par un idéal) que ces opérations ne dépendent pas des choix du vecteur v et v' dans les classes de congruences $v(\text{mod } U)$ et $v'(\text{mod } U)$.

1. Montrer que la multiplication externe

$$\bullet.\bullet : \begin{array}{ccc} K\times V/U & \mapsto & V/U \\ (\lambda, v(\text{mod } U)) & \mapsto & \lambda.v(\text{mod } U):=\lambda.v+U \end{array}$$

est bien définie et munit le quotient V/U d'une structure de K-EV.

2. Montrer que l'application

$$\bullet(\text{mod } U) : \begin{array}{ccc} V & \mapsto & V/U \\ v & \mapsto & v(\text{mod } U) \end{array}$$

est linéaire, surjéctive et de noyau égal à

$$\ker(\bullet(\text{mod } U))=U$$

3. Montrer que si V est de dimension finie il en est de même de V/U et que

$$\dim V/U = \dim V - \dim U$$

4. Soit $\varphi : V \to W$ une application linéaire et $U := \ker \varphi$. Montrer que si $v' \in v(\text{mod } U)$ alors

$$\varphi(v') = \varphi(v)$$

En déduire que si on pose pour toute classe $v(\text{mod } U)$:

$$\bar{\varphi}(v(\text{mod } U)) := \varphi(v)$$

on obtient une application bien définie

$$\bar{\varphi} : V/U \to W$$

Montrer que cette application est linéaire pour la structure de K-EV sur V/U définie précedemment.

5. Montrer que $\bar{\varphi} : V/U \to W$ est injective et que $\bar{\varphi}$ définit un isomorphisme du K-EV V/U sur son image $\varphi(V) \subset W$

Remarque 3.1. On sait que le noyau d'une application linéaire est un SEV. La question 2 montre réciproquement que tout SEV est le noyau d'une application linéaire convenable.

Remarque 3.2. Étant donné une application linéaire $\varphi : V \to W$ le fait que l'on ai un isomorphisme

$$\bar{\varphi} : V/\ker \varphi \simeq \varphi(V)$$

(qui est valable en dimension finie ou non) est la version précise du Thm. Noyau-Image. Ainsi ce théorème n'est que le premier théorème d'isomorphisme pour les espaces vectoriels.

Solution 7. 1. Commencons par montrer que la multiplication externe est bien définie. Soit donc v, v' deux représentants de la même classe de congruence modulo U. On a que $\forall \lambda \in K$, $\lambda.(v(\text{mod } U) = \lambda.v + U$ et $\lambda.(v'(\text{mod } U) = \lambda.v' + U$. Il suffit de montrer ainsi que $\lambda.v + U = \lambda.v' + U$. Ceci est vrai car $v - v' \in U \implies \lambda.(v - v') \in U$ car U est un SEV, et donc $\lambda.v$ est congru à $\lambda.v'$ modulo U.

V/U est déjà muni d'une structure de groupe additif. On à montré de plus qu'il y a une multiplication externe sur V/U. Il suffit donc de montrer que cette multiplication externe satisfait les axiomes d'un espace vectoriel.

Associativité : $\forall \lambda, \lambda' \in K$, $v(\text{mod } U) \in V/U$ on a

$$(\lambda.\lambda').v(\text{mod } U) = (\lambda.\lambda').v + U = \lambda.(\lambda'.v) + U = \lambda.(\lambda'.(v(\text{mod } U)))$$

Distributivité : $\forall \lambda, \lambda' \in K,\ v(\text{mod } U), v'(\text{mod } U) \in V/U$:

$$\begin{aligned}(\lambda+\lambda').v(\text{mod } U) &= (\lambda+\lambda').v + U \\ &= \lambda.v + \lambda'.v + U \\ &= \lambda.v(\text{mod } U) + \lambda'.v(\text{mod } U)\end{aligned}$$

$$\begin{aligned}\lambda.(v(\text{mod } U) + v'(\text{mod } U)) &= \lambda.((v+v')(\text{mod } U)) \\ &= \lambda.(v+v') + U \\ &= \lambda.v + U + \lambda.v' + U \\ &= \lambda.v(\text{mod } U) + \lambda.v'(\text{mod } U)\end{aligned}$$

Neutralité : $\forall v(\text{mod } U) \in V/U$:

$$1_K.(v(\text{mod } U)) = 1_K.v + U = v + U = v(\text{mod } U)$$

Donc V/U est bien un K-EV sous cette multiplication externe $\square$

2. $\forall \lambda \in K, v, v' \in V$:

$$(v + \lambda v')(\text{mod } U) = v(\text{mod U}) + \lambda.(v'(\text{mod } U))$$

par la définition des opérations sur V/U, et donc $\bullet(\text{mod } U)$ est linéaire. $\bullet(\text{mod } U)$ est surjéctive car $\forall v(\text{mod } U) \in V/U$, $v(\text{mod } U) = \bullet(\text{mod } U)(v)$. Finalement, $v \in \ker \bullet(\text{mod } U) \iff v(\text{mod } U) = 0(\text{mod } U) \iff v \in U$ donc $\ker \bullet(\text{mod } U) = U$ comme voulu $\square$

3. Par le théorème noyau image appliquée à $\bullet(\text{mod } U)$ et la partie précédente on a que
$$\dim V = \dim U + \dim V/U$$
ce qui est exactement ce quon devait montrer $\square$

4. $v' \in v(\text{mod } U) \iff v' - v \in U$ donc $\varphi(v'-v) = 0$ car $U = \ker \varphi$ et ainsi par linéarité de φ, $\varphi(v') = \varphi(v)$. Ainsi l'application $v\bar{p}hi$ est bien définie car on vient de voir que φ est invariante entr différents représentants de la même classe de congruence. On montre que $\bar{\varphi}$ est linéaire. $\forall \lambda \in K, v(\text{mod } U), v'(\text{mod } U) \in V/U$:

$$\begin{aligned}\bar{\varphi}(\lambda.(v(\text{mod } U)) + v'(\text{mod } U)) &= \bar{\varphi}((\lambda.v + v')(\text{mod } U)) \\ &= \varphi(\lambda.v + v') \\ &= \lambda.\varphi(v) + \varphi(v') \\ &= \lambda.\bar{\varphi}(v(\text{mod } U)) + \bar{\varphi}(v'(\text{mod } U))\end{aligned}$$

donc $\bar{\varphi}$ est bien linéaire pour la structure précedemment définie, comme voulu $\square$

5. Soit $v(\text{mod } U) \in \ker \bar{\varphi}$. Alors $\phi(v) = 0 \iff v \in U \iff v(\text{mod } U) = 0_{V/U}$. Ainsi $\bar{\varphi}$ est injéctive comme voulu et ainsi

$$\bar{\varphi} : V/U \to \bar{\varphi} = \phi(V) \subset W$$

est un isomorphisme $\square$

4 Le petit Théorème de Fermat

Exercice 8. Soit $p \geqslant 3$ un nombre premier impair et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps fini a p élements.

1. Montrer par récurrence que pour tout entier $n \geqslant 0$,

$$n^p - n \equiv 0(\text{mod } p)$$

(on pourra utiliser la formule du binôme de Newton)

2. Montrer que pour tout $x \in \mathbb{F}_p$ on a

$$x^p = x$$

et que pour tout $x \in \mathbb{F}_p^\times$ on a

$$x^{p-1} = 1$$

(ici on note 1 pour $1_{\mathbb{F}_p} = 1(\text{mod } p)$ et on note -1 pour son opposé).

Remarque 4.1. On peut montrer que si K est un corps fini de caractérsitique p (de sorte que K contient le corps $\mathbb{F}_p$ comme sous-corps premier) alors pour $x \in K$

$$x^p = x \implies x \in \mathbb{F}_p$$

Pour cela on dit (admet) que comme K est un corps, le polynôme (à coefficients dans $\mathbb{F}_p$) $P(X) = X^p - X$ est de degré $d = p$, la fonction polynomiale sur K $x \mapsto P(x) = x^p - x$ ne possède pas plus de d racines dans K (de solutions dans K de l'équation $P(x) = x^p - x = 0$) et comme $\mathbb{F}_p \subset K$ est déjà un ensemble de p racines, on les a toutes...

Solution 8. 1. Le cas $n = 0$ et $n = 1$ sont évidents. Considérons le cas $n = k + 1$, en supposant le théorème vrai pour $n = k$. On va montrer que $(k+1)^p \equiv k + 1(\text{mod } p)$. On a par la formule du binôme de Newton que

$$(k+1)^p = \sum_{j=0}^{p} \binom{p}{j} k^j = \sum_{j=0}^{p} \frac{p!}{j!(p-j)!} k^j$$

On a que $\frac{p!}{j!(p-j)!}$ est un entier divisible par p tant que $0 < j < p$ car p ne divise alors pas le dénominateur (car c'est un premier) et divise le numérateur, ce qui suffit pour dire (car p est premier) que $p|\binom{p}{j}$. Ainsi tout les coefficients de k^j pour $0 < j < p$ congruent à 0 mod p, et on obtient que

$$(k+1)^p \equiv k^p + 1 \equiv k + 1 (\text{mod } p)$$

par l'hypothèse de récurrence, comme on voulait le démontrer □

2. On a $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ donc il existe un entier n tel que $x = \pi(n)$ avec $\pi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ l'application quotient (un morphisme d'anneau). Ainsi par la partie précedente on obtient que $x^p - x = \pi(n^p - n) = 0$ et ainsi $x^p = x$ comme voulu. Si $x \in \mathbb{F}_p^\times$, alors x est inversible et on obtient

$$x^{-1}x^p = x^{-1}x \implies x^{p-1} = 1$$

comme voulu □

5 Encore des corps (pour les aficionad.a.os)

Exercice 9. On reprend les notations de l'exercice précedent. En particulier p est premier impair. On va étudier l'ensemble des carrés de $\mathbb{F}_p$:

$$(\mathbb{F}_p)^2 = \{z^2, z \in \mathbb{F}_p\}$$

L'élément nul $0_{\mathbb{F}_p} = 0^2_{\mathbb{F}_p}$ est toujours un carré il reste donc à étudier l'ensemble des carrés non-nuls. On va montrer que cet ensemble est non-vide et calculer son cardinal.

1. On note
$$(\mathbb{F}_p^\times)^2 = \{z^2, z \in \mathbb{F}_p^\times\}$$
l'ensemble des carrés de $\mathbb{F}_p^\times$. Montrer que $(\mathbb{F}_p^\times)^2$ est un sous-groupe du groupe multiplicatif $(\mathbb{F}_p^\times, .)$
2. Montrer que pour tout $x \in \mathbb{F}_p$ on a
$$x^2 - 1 = (x-1)(x+1)$$
et en déduire que si $x^2 = 1$ alors $x = \pm 1$.
3. Plus généralement, montrer que pour tout $z^2 \in (\mathbb{F}_p^\times)^2$
$$\{x \in \mathbb{F}_p^\times, x^2 = z^2\} = \{z, -z\}$$
Quel est le cardinal de cet ensemble ?

4. En déduire que
$$\left|(\mathbb{F}_p^\times)^2\right| = \frac{p-1}{2}$$
(on observera que $\mathbb{F}_p^\times$ est la réunion disjointe des sous-ensembles $\{x \in \mathbb{F}_p^\times, x^2 = z^2\}$ quand z^2 parcours $(\mathbb{F}_p^\times)^2$).
5. Comme p est impair, $\frac{p-1}{2}$ est un entier. Montrer que pour tout $z \in \mathbb{F}_p^\times$
$$z^{\frac{p-1}{2}} = \pm 1$$
(calculer $(z^{\frac{p-1}{2}})^2$)
6. En s'inspirant de la remarque ci-dessus, montrer que
$$\left|\{w \in \mathbb{F}_p^\times, w^{\frac{p-1}{2}} = +1\}\right| \leqslant \frac{p-1}{2}, \left|\{w \in \mathbb{F}_p^\times, w^{\frac{p-1}{2}} = -1\}\right| \leqslant \frac{p-1}{2}$$
et en déduire que
$$\left|\{w \in \mathbb{F}_p^\times, w^{\frac{p-1}{2}} = +1\}\right| = \left|\{w \in \mathbb{F}_p^\times, w^{\frac{p-1}{2}} = -1\right| = \frac{p-1}{2}$$
7. Montrer que
$$w \in (\mathbb{F}_p^\times)^2 \implies w^{\frac{p-1}{2}} = 1$$
et en déduire qu'en fait
$$(\mathbb{F}_p^\times)^2 = \{w \in \mathbb{F}_p^\times, w^{\frac{p-1}{2}} = 1\}$$
et que
$$\mathbb{F}_p^\times - (\mathbb{F}_p^\times)^2 = \{w \in \mathbb{F}_p^\times, w^{\frac{p-1}{2}} = -1\}$$
8. Montrer qu'il existe $w_0 \in \mathbb{F}_p^\times$ tel que $w_0 \notin \mathbb{F}_p^\times$ (ie. w_0 n'est pas un carré dans $\mathbb{F}_p^\times$) et que
$$\mathbb{F}_p^\times - (\mathbb{F}_p^\times)^2 = w_0.(\mathbb{F}_p^\times)^2 = \{w_0.z^2, z \in \mathbb{F}_p^\times\}$$
9. Montrer que $-1_{\mathbb{F}_p}$ est un carré dans $\mathbb{F}_p$ (il existe $z \in \mathbb{F}_p$ tel que $z^2 = -1_{\mathbb{F}_p}$) si et seulement si $p \equiv 1 (\mathrm{mod}\ 4)$

Solution 9. 1. Soient $z^2, w^2 \in (\mathbb{F}_p^\times)^2$ deux carrés de $\mathbb{F}_p$. On a que $(z^2)^{-1}w^2 = (z^{-1}w)^2$ donc par le critère de sous groupe, $(\mathbb{F}_p^\times)^2$ est un sous groupe de $(\mathbb{F}_p^\times, .)$ $\square$

2. Soit $x \in \mathbb{F}_p$. Alos $(x-1)(x+1) = x^2 - x + x - 1 = x^2 - 1$ par distributivité de la multiplication dans $\mathbb{F}_p$. Ainsi $x^2 = 1$ ssi $(x-1)(x+1) = 0$. Comme $\mathbb{F}_p$ est un anneaux intègre entre autre, on obtient que soit $x - 1 = 0$ ou $x + 1 = 0$ donc $x = \pm 1$ $\square$

3. On peut écrire de manière plus générale que $x^2 - z^2 = (x-z)(x+z)$ par la distributitivité de la multiplication et la commutativité dans $\mathbb{F}_p^\times$ $\square$. Ainsi par le même argument que précedemment, on obtient que les solutions de $x^2 = z^2$ sont $z, -z$. Cet ensemble est donc de cardinal 2 pour tout $z^2 \in (\mathbb{F}_p\times)$ (car $z \neq 0_{\mathbb{F}_p}$ et que c'est le seul élément qui satisfait $x = -x$ dans un corps de caracteristique $\neq 2$) $\square$
4. Notons que la relation $a \sim b \iff a^2 = b^2$ est une relation d'équivalence sur $\mathbb{F}_p^\times$. La classe de z sous cette relation est l'ensemble $\{x \in \mathbb{F}_p^\times, x^2 = z^2\}$ de la partie précédente. On peut donc écrire (comme pour l'indice) que

$$\mathbb{F}_p^\times = \bigsqcup_{z^2 \in (\mathbb{F}_p^\times)^2} \{x \in \mathbb{F}_p^\times, x^2 = z^2\} = \bigsqcup_{z^2 \in (\mathbb{F}_p^\times)^2} \{z, -z\}$$

   On obtient donc que

$$\left|\mathbb{F}_p^\times\right| = 2\left|(\mathbb{F}_p^\times)^2\right|$$

   Ainsi $\left|(\mathbb{F}_p^\times)^2\right| = \frac{p-1}{2}$ comme voulu $\square$
5. Par le petit théorème de Fermat (suivant soit d'un exercice précédent, soit du fait que $\mathbb{F}_p^\times$ est un groupe d'ordre $p-1$), on a que $\forall z \in \mathbb{F}_p,\ (z^{\frac{p-1}{2}})^2 = 1$. Ainsi par la partie 2, $z^{\frac{p-1}{2}} = \pm 1$ $\square$
6. On considère le polynôme $x^{\frac{p-1}{2}} - 1 \in \mathbb{F}_p[x]$. Ceci est un polynôme de degré $\frac{p-1}{2}$ et donc admet au plus $\frac{p-1}{2}$ racines sur $\mathbb{F}_p$. Ainsi

$$\left|\{w \in \mathbb{F}_p^\times, w^{\frac{p-1}{2}} = +1\}\right| \leqslant \frac{p-1}{2}$$

   De manière similaire,

$$\left|\{w \in \mathbb{F}_p^\times, w^{\frac{p-1}{2}} = -1\}\right| \leqslant \frac{p-1}{2}$$

   Ainsi par la question précédente, on a que

$$\left|\{w \in \mathbb{F}_p^\times, w^{\frac{p-1}{2}} = -1\}\right| = p - 1 - \left|\{z \in \mathbb{F}_p^\times, z^{\frac{p-1}{2}} = +1\}\right|$$

   et donc

$$\left|\{w \in \mathbb{F}_p^\times, w^{\frac{p-1}{2}} = +1\}\right| = \left|\{w \in \mathbb{F}_p^\times, w^{\frac{p-1}{2}} = -1\}\right| = \frac{p-1}{2}$$

   $\square$ **Méthode alternative (mais se basant sur un résultat non trivial)** : Il se trouve que $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$. En choisissant un générateur g de ce groupe, on a que $g^{\frac{p-1}{2}} = -1$ (car l'ordre de g est $p-1$). Alors on obtient que

$$(g^k)^{\frac{p-1}{2}} = \begin{cases} 1,\ k \equiv 0 (\mathrm{mod}\ 2) \\ -1,\ k \equiv 1 (\mathrm{mod}\ 2) \end{cases}$$

et chaque z^k est distinct donc on obtient directement que

$$\left|\{w \in \mathbb{F}_p^\times, w^{\frac{p-1}{2}} = +1\}\right| = \left|\{w \in \mathbb{F}_p^\times, w^{\frac{p-1}{2}} = -1\}\right| = \frac{p-1}{2}$$

□

7. Soit $w \in (\mathbb{F}_p^\times)^2$, alors $\exists z \in \mathbb{F}_p^\times$ tel que $w = z^2$ et on obtient que

$$(w^{\frac{p-1}{2}}) = (z^2)^{\frac{p-1}{2}} = z^{p-1} = 1$$

Mais alors on a que

$$\mathbb{F}_p^\times \subset \left|\{w \in \mathbb{F}_p^\times, w^{\frac{p-1}{2}} = +1\}\right|$$

et ces deux ensembles étant de même cardinalité on obtient égalité. Le deuxiême résultat suit de

$$\left|\{w \in \mathbb{F}_p^\times, w^{\frac{p-1}{2}} = -1\}\right| = \mathbb{F}_p^\times - \left|\{w \in \mathbb{F}_p^\times, w^{\frac{p-1}{2}} = 1\}\right| = \mathbb{F}_p^\times - (\mathbb{F}_p^\times)^2$$

□

8. On choisit $w_0 \in \mathbb{F}_p^\times$ tel que $w_0^{\frac{p-1}{2}} = -1$. Soit $z \in (\mathbb{F}_p^\times)^2$, alors $(w_0 z)^{\frac{p-1}{2}} = w_0^{\frac{p-1}{2}} z^{\frac{p-1}{2}} = -1 \cdot 1 = -1 \neq 1$ donc $w_0 z \in \mathbb{F}_p^\times - (\mathbb{F}_p^\times)^2$. Maintenant comme w_0 est inversible, l'application de multiplication à gauche par w_0 est une bijéction et donc $\left|w_0.(\mathbb{F}_p^\times)^2\right| = \frac{p-1}{2}$, et ainsi on obtient que

$$w_0.(\mathbb{F}_p^\times)^2 = \mathbb{F}_p^\times - (\mathbb{F}_p^\times)^2$$

□

9. Si $p \equiv 1 (\text{mod } 4)$ on a qu'il existe $k \in \mathbb{N}$ tel que $p = 4k + 1$. Alors $(-1_{\mathbb{F}_p})^{\frac{p-1}{2}} = (-1_{\mathbb{F}_p})^{2k} = 1_{\mathbb{F}_p}$ dans $\mathbb{F}_p$. Ainsi dans ce cas $-1_{\mathbb{F}_p}$ est un carré dans $\mathbb{F}_p$. Inversement, si $p \not\equiv 1 (\text{mod } 4)$ alors comme p est supposé impair on a que $p \equiv 3 (\text{mod } 4)$, et donc $\exists k \in \mathbb{N}$ tel que $p = 4k + 3$, mais alors $(-1_{\mathbb{F}_p})^{\frac{p-1}{2}} = (-1_{\mathbb{F}_p})^{2k+1} = -1_{\mathbb{F}_p}$ donc $-1_{\mathbb{F}_p}$ n'est pas un carré dans $\mathbb{F}_p$ □

Remarque 5.1. On peut donc déterminer si $w \in \mathbb{F}_p^\times$ est un carré ou pas en calculant sa puissance $w^{\frac{p-1}{2}}$ et en voyant si c'est $+1$ ou -1.

Par exemple prenons $p = 17$ et $w = 3 (\text{mod } 17)$. On a $\frac{p-1}{2} = 8$ et

$$w^8 = ((3^2)^2)^2$$

$$3^2 \equiv 9 (\text{mod } 17),\ 9^2 \equiv 81 (\text{mod } 17) \equiv 13 (\text{mod } 17)$$

$$13^2 \equiv 169 (\text{mod } 17) \equiv 16 (\text{mod } 17) \equiv -1 (\text{mod } 17)$$

et donc 3(mod 17) n'est pas un carré modulo 17. Remarquer que le fait d'écrire $8 = 2 \times 2 \times 2$ permet de calcular la puissance 8-ème en trois opérations. De la même manière pour $p = 23$, $\frac{p-1}{2} = 11$ on calculerait une puissance 11-ème en décomposant en base 2 :

$$w^1 1 = w^8 w^2 w = ((w^2)^2)^2 w^2 w$$

$$3^2 \equiv 9(\text{mod } 23),\ 9^2 \equiv 12(\text{mod } 23),\ 3^8 \equiv 12^2 \equiv 6(\text{mod } 23)$$

$$6.9.3 \equiv 1(\text{mod } 23)$$

de sorte que 3 est un carré modulo 23.

On pourrait se poser la question de connaitre les carrés modulo n pour n arbitraire. De tels calculs s'appelent des alculs de symboles de Legendre, et il y'a plusieurs résultats (comme celui que l'on vient de démontrer) qui rendent ces calculs plus simples.

Remarque 5.2. Le premier théoreme d'isomophisme a été utilisé implicitement dans la partie 4 : la relation $\sim$ est celle associée au quotient par le sous groupe normal $\{\pm 1\}$.

Remarque 5.3. On a donc montré que pour tout p premier impair, il existe un élément de $\mathbb{F}_p$ qui n'est pas un carré dans $\mathbb{F}_p$ (il en existe même $\frac{p-1}{2}$). Par les exercices 9 et 10 de la série précédent cela permet de construire un corps fini $\mathbb{F}_{p^2}$ de cardinal p^2 (comme sous-anneau de l'anneau $M_2(\mathbb{F}_p)$).

Exercice 10. Pour $p = 2$, tout élément de $\mathbb{F}_2$ est un carré, donc les exercices de la série précédente ne permettent pas de construire de corps fini à 4 élémenets. Voici une variante.

1. Pour $K = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ le corps à deux éléments, reprendre l'exercice 9 de la série 6 avec la matrice
$$I = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in M_2(\mathbb{F}_2)$$
et montrer que $\mathbb{F}_2[I]$ un anneau commutatif.
2. En utilisant le faut (le montrer) que l'équation $u^2 + u = 1$ n'a pas de solution dans $\mathbb{F}_2$ montrer que $\mathbb{F}_2[I]$ est un corps de cardinal 4. On le note $\mathbb{F}_4$.

Solution 10. 1. On rappel que $\mathbb{F}_2[I] = \{\lambda I_2 + \mu I : \lambda, \mu \in \mathbb{F}_2\}$. On montrer que $\mathbb{F}_2[I]$ est un sous-anneau de $M_2(\mathbb{F}_2)$. On sait que $\mathbb{F}_2[I]$ est un sous groupe additif engendré par I_2 et I. Ainsi il suffit de vérifier que le produit est stable. Soient $\lambda I_2 + \mu I, \lambda' I_2 + \mu' I \in \mathbb{F}_2[I]$.

$$(\lambda I_2 + \mu I)(\lambda' I_2 + \mu' I) = (\lambda\lambda' + \mu\mu') I_2 + (\lambda\mu' + \lambda'\mu + \mu\mu') I \in \mathbb{F}_2[I]$$

en utilisant le fait que $I^2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = I + I_2$. De plus $\mathbb{F}_2[I]$ est commutatif car I et I_2 commutent.

2. On a que $1^2+1=0$ et $0^2+0=0$ donc $u^2+u=1$ n'a pas de solution dans $\mathbb{F}_2$. Cependant cette équation a une solution dans $\mathbb{F}_2[I]$, notamment $u=I$. En particulier, I et $I+I_2$ sont inverses l'un de l'autre, et I_2 est son propre inverse. Comme $\mathbb{F}_2[I]=\{0_2, I_2, I, I+I_2\}$ on en déduit que chaque élément non nul est inversible et donc que $\mathbb{F}_2[I]$ est un corps à 4 éléments.

6 Exercice 9 avant modification :

Exercice 11. On reprend les notations de l'exercice précedent. En particulier p est premier impair. On va étudier l'ensemble des carrés de $\mathbb{F}_p$:

$$(\mathbb{F}_p)^2 = \{z^2, z \in \mathbb{F}_p\}$$

L'élément nul $0_{\mathbb{F}_p} = 0^2_{\mathbb{F}_p}$ est toujours un carré il reste donc à étudier l'ensemble des carrés non-nuls. On va montrer que cet ensemble est non-vide et calculer son cardinal.

1. On note
$$(\mathbb{F}_p^\times)^2 = \{z^2, z \in \mathbb{F}_p^\times\}$$
l'ensemble des carrés de $\mathbb{F}_p^\times$. Montrer que $(\mathbb{F}_p^\times)^2$ est un sous-groupe du groupe multiplicatif $(\mathbb{F}_p^\times, .)$
2. Montrer que pour tout $x \in \mathbb{F}_p$ on a
$$x^2 - 1 = (x-1)(x+1)$$
et en déduire que si $x^2=1$ alors $x = \pm 1$.
3. Comme p est impair, $\frac{p-1}{2}$ est un entier. Montrer que pour tout $z \in \mathbb{F}_p^\times$
$$z^{\frac{p-1}{2}} = \pm 1$$
(calculer $(z^{\frac{p-1}{2}})^2$)
4. En s'inspirant de la remarque ci-dessus, montrer que
$$\left|\{z \in \mathbb{F}_p^\times, z^{\frac{p-1}{2}} = +1\}\right| \leqslant \frac{p-1}{2}, \ \left|\{z \in \mathbb{F}_p^\times, z^{\frac{p-1}{2}} = -1\}\right| \leqslant \frac{p-1}{2}$$
et en déduire que
$$\left|\{z \in \mathbb{F}_p^\times, z^{\frac{p-1}{2}} = +1\}\right| = \left|\{z \in \mathbb{F}_p^\times, z^{\frac{p-1}{2}} = -1\}\right| = \frac{p-1}{2}$$
5. Montrer que
$$z \in (\mathbb{F}_p^\times)^2 \implies z^{\frac{p-1}{2}} = 1$$
On va montrer la réciproque.

6. Déduire des question précedents qu'il existe $z_0 \in \mathbb{F}_p^\times$ tel que $z_0 \notin (\mathbb{F}_p^\times)^2$ (ie. z_0 n'est pas un carré dans $\mathbb{F}_p^\times$) et qu'on a l'inclusion

$$z_0.(\mathbb{F}_p^\times)^2 = \{z_0.z^2, z \in \mathbb{F}_p^\times\} \subset \mathbb{F}_p^\times - (\mathbb{F}_p^\times)^2$$

7. En déduire que

$$|(\mathbb{F}_p^\times)^2| = |\mathbb{F}_p^\times - (\mathbb{F}_p^\times)^2| = \frac{p-1}{2}$$

et que

$$(\mathbb{F}_p^\times)^2 = \{z \in \mathbb{F}_p^\times, z^{\frac{p-1}{2}} = +1\}$$

$$\mathbb{F}_p^\times - (\mathbb{F}_p^\times)^2 = \{z \in \mathbb{F}_p^\times, z^{\frac{p-1}{2}} = -1\}$$

8. Montrer que $-1_{\mathbb{F}_p}$ est un carré dans $\mathbb{F}_p$ (il existe $z \in \mathbb{F}_p$ tel que $z^2 = -1_{\mathbb{F}_p}$) si et seulement si $p \equiv 1 (\text{mod } 4)$

Remarque 6.1. Le premier théorème d'isomorphisme permet d'aller beaucoup plus vite dans la question 7

Remarque 6.2. On a donc montré que pour tout premier impai, il existe un élément de $\mathbb{F}_p$ qui n'est pas un carré dans $\mathbb{F}_p$ (il en existe même $\frac{p-1}{2}$). Par les exercices 9 et 10 de la série précédente cela permet de construire un corps fini $\mathbb{F}_{p^2}$ de cardinal p^2 (comme sous-anneau de l'anneau $M_2(\mathbb{F}_p)$)

Solution 11.
1. Soient $z^2, w^2 \in (\mathbb{F}_p^\times)^2$ deux carrés de $\mathbb{F}_p$. On a que $(z^2)^{-1}w^2 = (z^{-1}w)^2$ donc par le critère de sous groupe, $(\mathbb{F}_p^\times)^2$ est un sous groupe de $(\mathbb{F}_p^\times, .)$ $\square$
2. Soit $x \in \mathbb{F}_p$. Alos $(x-1)(x+1) = x^2 - x + x - 1 = x^2 - 1$ par distributivité de la multiplication dans $\mathbb{F}_p$. Ainsi $x^2 = 1$ ssi $(x-1)(x+1) = 0$. Comme $\mathbb{F}_p$ est un anneaux intègre entre autre, on obtient que soit $x - 1 = 0$ ou $x + 1 = 0$ donc $x = \pm 1$ $\square$
3. Par le petit théorème de Fermat (suivant soit d'un exercice précédent, soit du fait que $\mathbb{F}_p^\times$ est un groupe d'ordre $p-1$), on a que $\forall z \in \mathbb{F}_p,\ (z^{\frac{p-1}{2}})^2 = 1$. Ainsi par la question précédente, $z^{\frac{p-1}{2}} = \pm 1$ $\square$
4. On considère le polynôme $x^{\frac{p-1}{2}} - 1 \in \mathbb{F}_p[x]$. Ceci est un polynôme de degré $\frac{p-1}{2}$ et donc admet au plus $\frac{p-1}{2}$ racines sur $\mathbb{F}_p$. Ainsi

$$\left|\{z \in \mathbb{F}_p^\times, z^{\frac{p-1}{2}} = +1\}\right| \leqslant \frac{p-1}{2}$$

De manière similaire,

$$\left|\{z \in \mathbb{F}_p^\times, z^{\frac{p-1}{2}} = -1\}\right| \leqslant \frac{p-1}{2}$$

Ainsi par la question précedente, on a que

$$\left|\{z \in \mathbb{F}_p^\times, z^{\frac{p-1}{2}} = -1\}\right| = p - 1 - \left|\{z \in \mathbb{F}_p^\times, z^{\frac{p-1}{2}} = +1\}\right|$$

et donc

$$\left|\{z \in \mathbb{F}_p^\times, z^{\frac{p-1}{2}} = +1\}\right| =, \ \left|\{z \in \mathbb{F}_p^\times, z^{\frac{p-1}{2}} = -1\}\right| = \frac{p-1}{2}$$

□ **Méthode alternative (mais se basant sur un résultat non trivial)** : Il se trouve que $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$. En choisissant un générateur z de ce groupe, on a que $z^{\frac{p-1}{2}} = -1$ (car l'ordre de z est $p-1$). Alors on obtient que

$$(z^k)^{\frac{p-1}{2}} = \begin{cases} 1, \ k \equiv 0 (\text{mod } 2) \\ -1, \ k \equiv 1 (\text{mod } 2) \end{cases}$$

et chaque z^k est distinct donc on obtient directement que

$$\left|\{z \in \mathbb{F}_p^\times, z^{\frac{p-1}{2}} = +1\}\right| = \left|\{z \in \mathbb{F}_p^\times, z^{\frac{p-1}{2}} = -1\}\right| = \frac{p-1}{2}$$

□

5. Soit $z \in (\mathbb{F}_p^\times)^2$, alors $\exists w \in \mathbb{F}_p^\times$ tel que $z = w^2$ et on obtient que

$$z^{\frac{p-1}{2}} = (w^2)^{\frac{p-1}{2}} = w^{p-1} = 1$$

comme voulu □

6. On choisit $z_0 \in \mathbb{F}_p^\times$ tel que $z_0^{\frac{p-1}{2}} = -1$: un tel z_0 existe par la parrtie 4, et n'est pas un carré par la partie 5. Soit $z \in (\mathbb{F}_p^\times)^2$, alors $(z_0 z)^{\frac{p-1}{2}} = z_0^{\frac{p-1}{2}} z^{\frac{p-1}{2}} = -1 \cdot 1 = -1 \neq 1$ donc $z_0 z \notin (\mathbb{F}_p^\times)^2$ comme voulu □

7. On considère le morphisme de groupe $\phi : \mathbb{F}_p^\times \to (\mathbb{F}_p^\times)^2$ défini par $x \mapsto x^2$. Par la partie 2, on a que $\ker \phi = \{\pm 1\}$. Ainsi par le premier théorème d'isomorphisme, on obtient que

$$\mathbb{F}_p^\times / \{\pm 1\} \cong (\mathbb{F}_p^\times)^2$$

et donc que $|(\mathbb{F}_p^\times)^2| = \frac{p-1}{2}$. Ainsi on obtient aussi que

$$|\mathbb{F}_p^\times - (\mathbb{F}_p^\times)^2| = p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$$

Par la partie 5,

$$(\mathbb{F}_p^\times)^2 \subset \{z \in \mathbb{F}_p^\times, z^{\frac{p-1}{2}} = +1\}$$

Comme ces deux ensembles ont la même cardinalité par la partie 4, on en déduit que

$$(\mathbb{F}_p^\times)^2 = \{z \in \mathbb{F}_p^\times, z^{\frac{p-1}{2}} = +1\}$$

On obtient l'autre résultat en notant que

$$\mathbb{F}_p^\times - \{z \in \mathbb{F}_p^\times, z^{\frac{p-1}{2}} = +1\} = \{z \in \mathbb{F}_p^\times, z^{\frac{p-1}{2}} = -1\}$$

par la partie 3 $\square$

8. Si $p \equiv 1(\text{mod } 4)$ on a qu'il existe $k \in \mathbb{N}$ tel que $p = 4k + 1$. Alors $(-1_{\mathbb{F}_p})^{\frac{p-1}{2}} = (-1_{\mathbb{F}_p})^{2k} = 1_{\mathbb{F}_p}$ dans $\mathbb{F}_p$. Ainsi dans ce cas $-1_{\mathbb{F}_p}$ est un carré dans $\mathbb{F}_p$. Inversement, si $p \not\equiv 1(\text{mod } 4)$ alors comme p est supposé impair on a que $p \equiv 3(\text{mod } 4)$, et donc $\exists k \in \mathbb{N}$ tel que $p = 4k + 3$, mais alors $(-1_{\mathbb{F}_p})^{\frac{p-1}{2}} = (-1_{\mathbb{F}_p})^{2k+1} = -1_{\mathbb{F}_p}$ donc $-1_{\mathbb{F}_p}$ n'est pas un carré dans $\mathbb{F}_p$ $\square$