Cyclotomie - TD - Correction

Salim Rostam
Complément d'algèbre pour l'agrégation, ENS Rennes

De nombreux exercices du Perrin sont corrigés dans *Exercices d'algèbre* de Pascal Ortiz. Certaines corrections se trouvent également dans le *Exercices de mathématiques pour l'agrégation* de S. Francinou et H. Gianella. Voir le tableau de correspondance des exos et des corrigés à la fin du Ortiz.

Exercice 1 (Groupe multiplicatif d'un corps fini, Perrin Théorème 2.7 p.74)**.** Soit k un corps et soit G un sous-groupe fini de $k^\times$.

1. Montrer que si $n \in \mathbb{N}^*$ alors $n = \sum_{d|n} \varphi(n)$.
2. En comptant les éléments d'ordre d de G pour $d \mid \#G$, montrer que G est cyclique.

Exercice 2 (Groupe multiplicatif d'un corps fini bis, Mercier *Cours de géométrie* Lemme 16 p.296)**.** Soit G un groupe et k un corps.

1. Si $x \in G$ est d'ordre ab, montrer que x^a est d'ordre b. *On a $(x^a)^b = 1$ donc l'ordre de x^a divise b, et si $(x^a)^k = 1$ alors $x^{ak} = 1$ donc ab divise ak donc b divise k.*

On suppose maintenant que G est un sous-groupe fini de $k^\times$. On note $n = \prod_{i=1}^r p_i^{\alpha_i}$ le cardinal de G.

2. Montrer que G possède un élément d'ordre $p_i^{\alpha_i}$ pour tout i. *Indication* : on pourra raisonner par l'absurde. *On suppose que G ne possède aucun élément d'ordre $p_i^{\alpha_i}$. Par la question précédente, l'ordre de tout élément $x \in G$ est donc de la forme $\prod p_j^{\beta_j}$ avec $\beta_i < \alpha_i$. Ainsi, les éléments de G sont tous racines du polynôme $X^{\frac{n}{p_i}} - 1 \in k[X]$, qui possède au plus $\frac{n}{p_i}$ racines puisque k est commutatif, donc $n \leq \frac{n}{p_i}$ ce qui est absurde.*
3. En déduire que G est cyclique. *Pour chaque i on a un élément $x_i \in G$ d'ordre $p_i^{\alpha_i}$. Puisque les p_i sont distincts, ils sont premiers entre eux donc puisque G est commutatif (car k l'est) on en déduit que $x_1 \cdots x_r$ est d'ordre $p_1^{\alpha_1} \cdots p_r^{\alpha_r} = n$ ce qui conclut.*

Exercice 3 (Perrin exo 4.3 p.92)**.** Montrer que Φ_n est un polynôme réciproque si $n \geq 2$, c'est-à-dire $\Phi_n(X) = X^{\deg \Phi_n} \Phi_n(\frac{1}{X})$. *En utilisant le fait que $\mu_n^\times(\mathbb{C})$ est stable par*

l'application $\zeta \mapsto \zeta^{-1}$, on obtient

$$\begin{aligned}\Phi_n(X) &= \prod_{\zeta \in \mu_n^\times(\mathbb{C})} (X - \zeta) \\ &= \prod_{\zeta} (-\zeta X)\left(\frac{1}{X} - \zeta^{-1}\right) \\ &= (-1)^{\varphi(n)} X^{\varphi(n)} \prod_{\zeta} \zeta \prod_{\zeta}\left(\frac{1}{X} - \zeta^{-1}\right) \\ &= (-1)^{\varphi(n)} X^{\varphi(n)} \Phi_n\left(\frac{1}{X}\right) \prod_{\zeta \in \mu_n^\times(\mathbb{C})} \zeta.\end{aligned}$$

L'application $\mu_n^\times(\mathbb{C}) \to \mu_n^\times(\mathbb{C})$ donnée par $\zeta \mapsto \zeta^{-1}$ n'a pas de point fixe sauf si $n = 2$, ainsi si $n > 2$ on a d'une part $\varphi(n) = \#\mu_n^\times(\mathbb{C})$ pair et $\prod_{\zeta \in \mu_n^\times(\mathbb{C})} \zeta = 1$, d'où $\Phi_n(X) = X^{\varphi(n)}\Phi_n\left(\frac{1}{X}\right)$. Si maintenant $n = 2$ on a $\mu_2^\times(\mathbb{C}) = \{-1\}$ donc on obtient également $\Phi_2(X) = X^{\varphi(2)}\Phi_2\left(\frac{1}{X}\right)$.

Exercice 4 (Fonction indicatrice d'Euler)**.**

1. Si m et n sont deux entiers premiers entre eux, montrer que $\varphi(mn) = \varphi(m)\varphi(n)$. *Il suffit de remarquer que par le théorème chiniois on a $(\mathbb{Z}/mn\mathbb{Z})^\times \simeq (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$.*
2. Si p est premier et $\alpha \geq 1$, montrer que $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. *Les entiers de $\{1, \dots, p^\alpha\}$ qui ne sont pas premiers avec p^α sont exactement les multiples de p, car p est premier. On conclut puisqu'il y a $p^{\alpha-1}$ multiples de p dans $\{1, \dots, p^\alpha\}$.*
3. En déduire que si $n = \prod_{i=1}^r p_i^{\alpha_i}$ alors $\varphi(n) = \prod_{i=1}^r p_i^{\alpha_i - 1}(p_i - 1) = n\prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$. *Par la question (1) on a $\varphi(n) = \prod_{i=1}^r \varphi(p_i^{\alpha_i})$. Par la question précédente, on obtient*

$$\varphi(n) = \prod_{i=1}^r p_i^{\alpha_i} - p_i^{\alpha_i - 1} = \prod_{i=1}^r p_i^{\alpha_i}(1 - p_i^{-1}) = n\prod_{i=1}^r (1 - p_i^{-1}).$$

4. (Ortiz III.35 p.169) Soit $N \in \mathbb{N}^*$. Montrer que $\{n \in \mathbb{N}^* : \varphi(n) \leq N\}$ est fini. *Soit n tel que $\varphi(n) \leq N$. Si p est un facteur premier de n, par la question précédente on sait que $p - 1 \mid \varphi(n)$ donc $p \leq N$. Ainsi, toujours par la question précédente, avec $C \coloneqq \prod_{k=1}^N \left(1 - \frac{1}{k}\right) > 0$ on a $\varphi(n) \geq nC$ donc $n \leq NC^{-1}$.*

Exercice 5 (Perrin exo 4.9 p.92)**.** Soit K une extension finie de $\mathbb{Q}$. Montrer que K ne possède qu'un nombre fini de racines de l'unité. *Indication* : on pourra utiliser la question 4 de l'Exercice 4. *Si $\zeta \in K$ est une racine primitive n-ième de l'unité alors K contient $\mathbb{Q}(\zeta)$. Puisque $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$, on a par la formule de multiplicativité des degrés que $[K : \mathbb{Q}] \geq \varphi(n)$. On conclut puisque par l'Exercice 4 il n'y a qu'un nombre fini de tels n.*

Exercice 6 (Perrin exo 4.10 p.92)**.** Trouver les entiers d sans facteur carré tel que $\mathbb{Q}(\sqrt{d})$ contienne d'autres racines de l'unité que 1 et -1. *Indication* : on pourra utiliser l'Exercice 4. *Si $\mathbb{Q}(\sqrt{d})$ contient une racine primitive n-ième ζ avec $n > 2$ alors comme dans l'Exercice 5 on a $\varphi(n) \leq [\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$. Par l'Exercice 4 on a donc $\prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) \leq 2$ donc $p_i \in \{2, 3\}$, $\alpha_2 \leq 2$ et $\alpha_3 \leq 1$. De plus, si $\alpha_2 = 2$ alors $\alpha_3 = 0$ donc il reste les valeurs suivantes (rappelons que $n \neq 2$) :*

α_2	α_3	n	$\varphi(n)$
2	0	4	2
1	1	6	2
0	1	3	2

.

Des racines sont par exemple j pour $n = 3$, i pour $n = 4$ et $-j$ pour $n = 6$. Ainsi, puisque $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\zeta)$ on a $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\zeta)$ (par le degré) donc les extensions recherchées sont $\mathbb{Q}(i)$ et $\mathbb{Q}(i\sqrt{3})$ i.e. $d \in \{-1, -3\}$.

Exercice 7 (Perrin exo 4.14 p.93)**.** Soit $n \geq 2$. On veut montrer une version faible du théorème de Dirichlet, à savoir : il existe une infinité de nombres premiers congrus à 1 modulo n.

1. Montrer qu'un nombre premier p est congru à 1 modulo n si et seulement si $\mathbb{F}_p$ possède une racine primitive n-ième de l'unité. *Si $p \equiv 1 \pmod{n}$ alors $n \mid (p-1)$ donc $\mathbb{F}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ possède un élément d'ordre n (par exemple $\frac{p-1}{n}$) donc $\mathbb{F}_p$ possède une racine primitive n-ième. Réciproquement, si $\mathbb{F}_p$ possède une racine primitive n-ième alors $\mathbb{F}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ possède un élément d'ordre n donc $n \mid (p-1)$ par le théorème de Lagrange.*
2. (a) Montrer que l'on peut trouver $k \geq n$ tel que $\Phi_n(k!) \neq 0, \pm 1$. *Puisque Φ_n n'est pas constant, les polynômes Φ_n et $\Phi_n \pm 1$ ont un nombre fini de racines. Pour k assez grand (que l'on peut donc choisir $\geq n$) on a donc $\Phi_n(k!) \neq 0, \pm 1$.*

   On choisit un tel k. Soit p un facteur premier de $\Phi_n(k!)$.

   (b) Montrer que $p > k$. *Puisque $\Phi_n \mid X^n - 1$ dans $\mathbb{F}_p[X]$, on en déduit que $p \mid (k!)^n - 1$. Si $p \leq k$ alors $p \mid k!$ et donc $p \mid 1$ ce qui est impossible.*

   (c) Montrer que $k!$ est une racine primitive n-ième de l'unité dans $\mathbb{F}_p$. *Puisque $k!$ est racine de Φ_n dans $\mathbb{F}_p$ on en déduit par définition que $k!$ est une racine primitive n-ième de l'unité dans $\mathbb{F}_p$, c'est-à-dire $k!$ est d'ordre n dans $\mathbb{F}_p^\times$.*
3. Conclure. *Pour $k \geq n$ assez grand, on a trouvé un nombre premier $p > k$ tel que $k!$ est une racine primitive de l'unité dans $\mathbb{F}_p$, en particulier $p \equiv 1 \pmod{n}$ par la question 1. On peut donc trouver des nombres premiers congrus à 1 modulo n aussi grand que possible, il y en a donc une infinité.*

Exercice 8 (Perrin exos 4.2 p.92 et 4.11 p.93)**.** Soit $n \geq 2$.

1. Rappeler l'expression de Φ_1. *Par définition $\Phi_1 = X - 1$.*
2. Calculer $\Phi_n(0)$. *Via la définition de Φ_n on a $\Phi_n(0) = \prod_{\zeta \in \mu_n^\times(\mathbb{C})}(-\zeta) = (-1)^{\varphi(n)} \prod_{\zeta \in \mu_n^\times(\mathbb{C})} \zeta$. Par nos calculs de l'Exercice 3 on obtient alors $\Phi_n(0) = 1$.*

3. Calculer $\Phi_n(1)$. *On a* $X^{n-1}+\cdots+X+1=\prod_{\substack{d|n\\ d\neq 1}}\Phi_d(X)$ *donc* $n=\prod_{\substack{d|n\\ d\neq 1}}\Phi_d(1)$. *Ainsi, si* $n=p$ *est premier alors* $\Phi_p(1)=p$, *et si* $\alpha\geq 2$ *alors* $p^\alpha=\prod_{\beta=1}^{\alpha}\Phi_{p^\beta}(1)$ *donc* $\Phi_{p^\alpha}(1)=p$ *par récurrence (sur* α*). Si maintenant* $n=\prod_{i=1}^{r}p_i^{\alpha_i}$ *avec* $r\geq 2$ *alors on trouve*

$$1=\prod_{\substack{d|n\\ d\neq 1\\ d\notin\{p_i,\dots,p_i^{\alpha_i}\}\,\forall i}}\Phi_d(1),$$

donc $\Phi_n(1)=1$ *par récurrence.*

4. Montrer que $\Phi_{2n}(X)=\begin{cases}\Phi_n(-X), & \text{si } n \text{ est impair,}\\ \Phi_n(X^2), & \text{si } n \text{ est pair.}\end{cases}$ *On suppose d'abord* n *est impair. Si* $\zeta\in\mu_n^\times(\mathbb{C})$ *alors* $-\zeta$ *est d'ordre* $2n$ *puisque* $2\wedge n=1$ *(et* $\mathbb{C}^\times$ *commutatif !) donc* $-\zeta\in\mu_{2n}^\times(\mathbb{C})$. *Réciproquement, si* $\xi\in\mu_{2n}^\times(\mathbb{C})$ *alors* $(\xi^n)^2=1$ *donc* $\xi^n=\pm 1$ *donc* $\xi^n=-1$ *puisque* ξ *n'est pas d'ordre* n. *Ainsi, puisque* n *est impair on a* $(-\xi)^n=-\xi^n=1$. *De plus,* n *est exactement l'ordre de* $-\xi\in\mathbb{C}^\times$ *puisque si* $(-\xi)^k=1$ *alors* $\xi^{2k}=(-\xi)^{2k}=1$ *donc* $n\mid k$ *puisque* $\xi\in\mathbb{C}^\times$ *est d'ordre* $2n$. *Finalement, si* n *est impair l'application*

$$\left|\begin{array}{ccc}\mu_n^\times(\mathbb{C}) & \longrightarrow & \mu_{2n}^\times(\mathbb{C})\\ \zeta & \longmapsto & -\zeta\end{array}\right.,$$

est une bijection (au passage on obtient $\varphi(n)=\varphi(2n)$*), donc on obtient, en utilisant le fait que* $\varphi(n)$ *est pair (voir Exercice 3)*

$$\begin{aligned}\Phi_n(-X)&=\prod_{\zeta\in\mu_n^\times(\mathbb{C})}(-X-\zeta)\\ &=\prod_{\zeta\in\mu_n^\times(\mathbb{C})}(X+\zeta)\\ &=\prod_{\zeta\in\mu_{2n}^\times(\mathbb{C})}(X-\zeta)\\ &=\Phi_{2n}(X).\end{aligned}$$

On suppose maintenant que n *est pair. De façon similaire au cas précédent, on montre que l'application*

$$\left|\begin{array}{ccc}\mu_{2n}^\times(\mathbb{C}) & \longrightarrow & \mu_n^\times(\mathbb{C})\\ \zeta & \longmapsto & \zeta^2\end{array}\right.,$$

est surjective. De plus, chaque élément de $\mu_n^\times(\mathbb{C})$ *possède exactement deux antécédents (*$\zeta\in\mu_n^\times(\mathbb{C})$ *est non nul et* $\mathbb{C}$ *étant de caractéristique différente de* 2*). Si* $\zeta\in\mu_{2n}^\times(\mathbb{C})$ *est l'antécédent de* $\xi\in\mu_n^\times(\mathbb{C})$ *alors* $-\zeta$ *est l'autre antédédent. En*

désignant par $\sqrt{\xi}$ un antécédent de $\xi \in \mu_n^\times(\mathbb{C})$, on obtient

$$\begin{aligned}\Phi_n(X^2) &= \prod_{\xi\in\mu_n^\times(\mathbb{C})} (X^2-\xi)\\ &= \prod_{\xi\in\mu_n^\times(\mathbb{C})} (X^2-(\sqrt{\xi})^2)\\ &= \prod_{\xi\in\mu_n^\times(\mathbb{C})} (X-\sqrt{\xi})(X+\sqrt{\xi})\\ &= \prod_{\zeta\in\mu_{2n}^\times(\mathbb{C})} (X-\zeta)\\ &= \Phi_{2n}(X).\end{aligned}$$

5. En déduire $\Phi_n(-1)$. *Si n est impair, on a $\Phi_n(-1) = \Phi_{2n}(1)$ donc puisque $2n$ possède au moins deux facteurs premiers distincts (rappelons que $n \geq 2$) on obtient $\Phi_n(-1) = 1$. On suppose donc que n est pair et on écrit $n = 2m$. Si $m = 1$ alors $n = 2$ et $\Phi_2 = X + 1$ donc $\Phi_2(-1) = 0$. On suppose donc maintenant $m > 1$. Si m est impair alors $\Phi_n(-1) = \Phi_{2m}(-1) = \Phi_m(-(-1)) = \Phi_m(1)$, et si m est pair alors $\Phi_n(-1) = \Phi_{2m}(-1) = \Phi_m((-1)^2) = \Phi_m(1)$. Ainsi, dans tous les cas on a $\Phi_n(-1) = \Phi_m(1)$, donc $\Phi_n(-1) = 1$ si $m = \frac{n}{2}$ possède au moins deux facteurs premiers distincts et $\Phi_n(-1) = p$ si $m = \frac{n}{2} = p^\alpha$.*

Exercice 9. L'objectif de cet exercice est de déterminer le coefficient de degré $\varphi(n) - 1$ de Φ_n, noté $m(n)$.

1. (Perrin exo 4.1 p.91.) Soit p premier et $\alpha \geq 2$.
   (a) Montrer que $m(p) = 1$. *On a $X^p - 1 = \Phi_p\Phi_1$ donc $\Phi_p = \frac{X^p-1}{X-1} = X^{p-1} + \cdots + X + 1$ donc $m(p) = 1$.*
   (b) Montrer que $\Phi_{p^\alpha}(X) = \frac{X^{p^\alpha}-1}{X^{p^{\alpha-1}}-1}$. *On vient de voir que la formule est vraie pour $\alpha = 1$. Par récurrence, si $\alpha \geq 2$ on obtient*

$$\Phi_{p^\alpha}(X) = \frac{X^{p^\alpha}-1}{X-1}\prod_{i=1}^{\alpha-1}\Phi_{p^i}^{-1}(X) = \frac{X^{p^\alpha}-1}{X-1}\prod_{i=1}^{\alpha-1}\frac{X^{p^{i-1}}-1}{X^{p^i}-1} = \frac{X^{p^\alpha}-1}{X^{p^{\alpha-1}}-1}.$$

   (c) En déduire que $\Phi_{p^\alpha}(X) = \Phi_p(X^{p^{\alpha-1}})$. *Découle de la formule précédente et de $\Phi_p = \frac{X^p-1}{X-1}$.*
   (d) En déduire que $m(p^\alpha) = 0$. *Par l'égalité précédente, les seules puissances de X qui apparaissent dans $\Phi_{p^\alpha}(X)$ sont de la forme $X^{ip^{\alpha-1}}$ avec $i \in \{0, \ldots, p-1\}$. Le coefficient de plus haut degré est atteint pour $i = p-1$ et vaut bien $(p-1)p^{\alpha-1} = \varphi(p^\alpha)$ (par l'Exercice 4), et pour $i = p-2$ on obtient $(p-2)p^{\alpha-1} = (p-1)p^{\alpha-1} - p^{\alpha-1} = \varphi(p^\alpha) - p^{\alpha-1} < \varphi(p^\alpha) - 1$ puisque $\alpha \geq 2$ et $p \geq 2$. On en déduit que $\Phi_{p^\alpha}(X)$ ne possède pas de terme de degré $\varphi(p^\alpha) - 1$ et donc $m(p^\alpha) = 0$.*

2. (Combes *Algèbre et géométrie* exo 10.10 p.227.) Soit $n \geq 2$ et soit $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ sa décomposition en facteurs premiers ($\alpha_i \geq 1$).

   (a) Montrer que l'application

   $$\left| \begin{array}{ccc} \mu_{p_1^{\alpha_1}}(\mathbb{C}) \times \cdots \times \mu_{p_r^{\alpha_r}}(\mathbb{C}) & \longrightarrow & \mu_n(\mathbb{C}) \\ (\zeta_1, \ldots, \zeta_r) & \longmapsto & \zeta_1 \cdots \zeta_r \end{array} \right. ,$$

   est un isomorphisme. *L'application est bien définie car $\mathbb{C}^\times$ est commutatif et pour la même raison c'est bien un morphisme. Maintenant si $\zeta_i \in \mu_{p_i^{\alpha_i}}(\mathbb{C})$ sont tels que $\zeta_1 \cdots \zeta_r = 1$ alors l'ordre de $\zeta_r^{-1} = \zeta_1 \cdots \zeta_{r-1}$ divise $p_r^{\alpha_r}$ et $\prod_{i=1}^{r-1} p_i^{\alpha_i}$ donc divise 1 donc $\zeta_r = 1$, et de proche en proche (ou par récurrence) on trouve $\zeta_1 = \cdots = \zeta_r = 1$. Finalement, le morphisme est injectif, et est donc un isomorphisme car les groupes ont le même cardinal n.*

   (b) En déduire que $m(n) = (-1)^{r-1} \prod_{i=1}^{r} m(p_i^{\alpha_i})$. *Par la question précédente, on sait que l'application*

   $$\left| \begin{array}{ccc} \mu^\times_{p_1^{\alpha_1}}(\mathbb{C}) \times \cdots \times \mu^\times_{p_r^{\alpha_r}}(\mathbb{C}) & \longrightarrow & \mu_n^\times(\mathbb{C}) \\ (\zeta_1, \ldots, \zeta_r) & \longmapsto & \zeta_1 \cdots \zeta_r \end{array} \right. ,$$

   est une bijection. On a $\Phi_n = \prod_{\zeta \in \mu_n^\times(\mathbb{C})} (X - \zeta)$ donc (en omettant les « $(\mathbb{C})$ » pour plus de lisibilité)

   $$\begin{aligned} m(n) &= -\sum_{\zeta \in \mu_n^\times} \zeta \\ &= -\sum_{i=1}^{r} \sum_{\zeta_i \in \mu^\times_{p_i^{\alpha_i}}} \zeta_1 \cdots \zeta_r \\ &= -\prod_{i=1}^{r} \left(\sum_{\zeta_i \in \mu^\times_{p_i^{\alpha_i}}} \zeta_i \right) \\ &= -\prod_{i=1}^{r} \left(-m(p_i^{\alpha_i}) \right) \\ &= (-1)^{r-1} \prod_{i=1}^{r} m(p_i^{\alpha_i}). \end{aligned}$$

   (c) En déduire que $m(n) = -\mu(n)$, où $\mu : \mathbb{N}^* \to \{-1, 0, 1\}$ est la *fonction de Möbius*, donnée par

   $$\mu(n) = \begin{cases} 0, & \text{si } n \text{ possède un facteur carré,} \\ (-1)^s, & \text{sinon, où } s \text{ est le nombre de facteurs premiers de } n. \end{cases}$$

   Par la question 1 et l'égalité précédente, on sait que $m(n) = 0$ si n possède un facteur multiple et $m(n) = (-1)^{r-1}$ sinon. On conclut.

Exercice 10 (Théorème de Wedderburn, Perrin Théorème 4.9 p.82)**.** Soit K un anneau à division (*i.e.* K est un anneau et $K^* \coloneqq K \setminus \{0\}$ est un groupe) fini. On suppose que K n'est pas commutatif. Soit

$$Z \coloneqq \{x \in K : xy = yx \text{ pour tout } y \in K\},$$

le centre de K.

1. Montrer que Z est un sous-corps de K, commutatif et de cardinal $q \geq 2$. *C'est bien un sous-corps car :*
   - $0, 1 \in Z$*, en particulier* $q \geq 2$ *;*
   - Z *est stable par* $+$ *et par opposé ;*
   - $Z \setminus \{0\}$ *est stable par* $*$ *et par inversion.*

   Finalement, Z *est commutatif par définition.*
2. Montrer que $\#K = q^n$ pour un certain $n \geq 2$. *K est un Z-espace vectoriel de dimension finie (car K est fini) donc $\#K$ est une puissance de $\#Z$ (prendre une Z-base de K). On a donc $\#K = q^n$ pour $n \geq 1$, mais $K \supsetneq Z$ puisque K n'est pas commutatif donc $n \geq 2$.*

On considère l'action de K^* sur lui-même par conjugaison. Pour $x \in K^*$ on note $\omega(x)$ son orbite et on définit $K_x \coloneqq \{y \in K : xy = xy\}$ de sorte que $K_x^* = K_x \setminus \{0\}$ est le centralisateur de x.

3. Montrer que K_x est un sous-corps de K. Est-il commutatif ? *On montre comme avant que K_x est un sous-corps de K, et il n'y a à priori pas de raison pour que K_x soit commutatif.*
4. Montrer que $\#K_x = q^d$ pour un certain $d \geq 1$. *On a $Z \subseteq K_x$ donc comme avant, le corps K_x est un Z-espace vectoriel de dimension finie donc $\#K_x$ est une puissance de $\#Z$.*
5. Montrer que $q^d - 1$ divise $q^n - 1$ et en déduire que $d \mid n$. *On sait que $\#K_x^\times$ divise $\#K^*$ puisque K_x^* est un sous-groupe de K^* (on peut aussi utiliser la relation orbite-stabilisateur). On trouve donc que $k \coloneqq q^d - 1$ divise $q^n - 1$. Ainsi, on a $q^n - 1 \equiv 0 \pmod{k}$ donc $q^n \equiv 0 \pmod{k}$ donc l'ordre de q dans $\mathbb{Z}/k\mathbb{Z}$ divise n, donc $d \mid n$ puisque cet ordre est d. (En effet, on a $q^d \equiv 1 \pmod{k}$ par définition de k et si $q^a \equiv 1 \pmod{k}$ alors $q^d - 1$ divise $q^a - 1$ donc $d \leq a$.)*
6. Montrer que $\#\omega(x) = \frac{q^n-1}{q^d-1}$ et en déduire que

$$\#\omega(x) = \prod_{\substack{m \mid n \\ m \nmid d}} \Phi_m(q).$$

   La première égalité vient de la relation orbite-stabilisateur, puisque K_x^* est exactement le stabilisateur de $x \in K^*$. Puisque $d \mid n$, si $m \mid d$ alors $m \mid n$ donc on obtient

$$\#\omega(x) = \frac{\prod_{m \mid n} \Phi_m(q)}{\prod_{m \mid d} \Phi_m(q)} = \prod_{\substack{m \mid n \\ m \nmid d}} \Phi_m(q).$$

7. Montrer qu'il existe $r \geq 1$ et $d_1, \ldots, d_r$ des diviseurs stricts de n tel que
$$q^n - 1 = q - 1 + \sum_{i=1}^{r} \frac{q^n - 1}{q^{d_i} - 1}.$$
Puisque K^* n'est pas commutatif, il existe des orbites non réduites à un point. Si $r \geq 1$ est le nombre d'orbites non réduites à un point, soit $x_1, \ldots, x_r$ des représentants de ces orbites. Par les questions précédentes on sait que $\#K_{x_i} = q^{d_i}$ et $\#\omega(x_i) = \frac{q^n-1}{q^{d_i}-1}$ pour $d_i \geq 1$ divisant de n. Puisque $\#\omega(x_i) > 1$ on a $d_i < n$, ainsi d_i est un diviseur strict de n. Par la formule des classes on a
$$K^* = Z^* \sqcup \bigsqcup_{i=1}^{r} \omega(x_i),$$
donc
$$q^n - 1 = q - 1 + \sum_{i=1}^{r} \frac{q^n - 1}{q^{d_i} - 1},$$
ce qui conclut.
8. En déduire que $\Phi_n(q)$ divise $q - 1$ et $|\Phi_n(q)| \leq q - 1$. *On sait que $\Phi_n(q)$ divise $q^n - 1$, de plus $\Phi_n(q)$ divise chaque $\frac{q^n-1}{q^{d_i}-1}$ par la question 6 (puisque $n \nmid d_i$ puisque $d_i < n$). Ainsi, par l'égalité de la question précédente on obtient $\Phi_n(q)$ divise $q - 1$ donc $|\Phi_n(q)| \leq |q - 1|$.*
9. Soit $\zeta \in \mathbb{C}$ de module 1 avec $\zeta \neq 1$. Montrer que $|q - \zeta| > q - 1$. *L'inégalité se voit sur un dessin, on peut aussi dire que $|q - \zeta| \geq q - \mathrm{Re}(\zeta) > q - 1$ puisque $\mathrm{Re}(\zeta) < 1$ par hypothèse.*
10. En déduire que l'inégalité de la question 8 est impossible. *On a $\Phi_n(q) = \prod_{\zeta \in \mu_n^\times(\mathbb{C})}(q - \zeta)$. Puisque $n \geq 2$, on a $1 \notin \mu_n^\times(\mathbb{C})$ et donc par la question précédente on obtient $|\Phi_n(q)| > |q - 1|^{\varphi(n)}$. Puisque $q \geq 2$ et $\varphi(n) \geq 1$ on obtient donc $|\Phi_n(q)| > q - 1$, ce qui contredit l'inégalité $|\Phi_n(q)| \leq q - 1$ de la question 8.*
11. Conclure. *L'hypothèse initiale est donc fausse, donc K est commutatif. Ainsi, on a montré que tout anneau à division fini est commutatif, autrement dit « tout corps fini est commutatif ».*

Exercice 11 (Demazure *Cours d'algèbre* Proposition 5.16 p.119)**.** Soit p un nombre premier impair. On considère l'anneau $A \coloneqq \mathbb{F}_p[X]/\langle X^4 + 1\rangle$ et on note α la classe de X.

1. Montrer que 2 est inversible dans A. *On a $p \neq 2$ donc 2 est inversible dans $\mathbb{F}_p$ donc dans A.*
2. Montrer que α est inversible dans A et que $\alpha^{-1} = -\alpha^3$. *On a $\alpha^4 = -1$ par définition donc α est inversible et $\alpha^{-1} = -\alpha^3$.*
3. On note $\beta \coloneqq \alpha + \alpha^{-1}$. Montrer que $\beta^2 = 2$ et en déduire que $\beta \in A^\times$. *On a $\beta^2 = \alpha^2 + \alpha^{-2} + 2 = \alpha^{-2}(\alpha^4 + 1) + 2 = 2$. On conclut par 1.*
4. En déduire que $\left(\frac{2}{p}\right) = \frac{\beta^p}{\beta}$ dans A. *Dans A on a $\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} = \beta^{p-1} = \frac{\beta^p}{\beta}$.*

5. Montrer que $\alpha^p = \begin{cases} \alpha^{\pm 1}, & \text{si } p \equiv \pm 1 \pmod 8, \\ \alpha^{\pm 3} = -\alpha^{\mp 1}, & \text{sinon } (p \equiv \pm 3 \pmod 8). \end{cases}$ *Écrivons* $p = 8k + r$ *avec* $k \geq -1$ *et* $r \in \{-3, \ldots, 4\}$*, en remarquant que* r *est nécessairement impair puisque* p *l'est. On a* $\alpha^4 = -1$ *donc* $\alpha^8 = 1$ *donc (rappelons que* α *est inversible)* $\alpha^p = \alpha^r$*. On conclut en utilisant l'égalité de la question 2.*

6. En déduire que $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ dans $\mathbb{Z}$. *D'après la question 4 et en utilisant le morphisme de Frobenius, on obtient*

$$\left(\frac{2}{p}\right) = \frac{\beta^p}{\beta} = \frac{\alpha^p + \alpha^{-p}}{\alpha + \alpha^{-1}} = \begin{cases} 1, & \text{si } p \equiv \pm 1 \pmod 8, \\ -1, & \text{sinon } (p \equiv \pm 3 \pmod 8), \end{cases}$$

par la question précédente. C'est une égalité dans A*, mais ce ses éléments valent* ± 1 *donc par la question 1 on en déduit que c'est une égalité dans* $\mathbb{Z}$*. On conclut puisque* $(\pm 1)^2 - 1 = 0 \pmod 8$ *et* $(\pm 3)^2 - 1 = 8 = 0 \pmod 8$*.*

Exercice 12 (Demazure *Cours d'algèbre* fin du §5.2.3 p.122)**.**

1. Soit p un nombre premier impair.
   (a) On suppose ici $p > 3$. Montrer que 3 est un carré modulo p si et seulement si $p \equiv \pm 1 \pmod{12}$. *Par la loi de réciprocité quadratique, on a* $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{3-1}{2}\frac{p-1}{2}} = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}$*. Puisque* 1 *est un carré modulo* 3 *et* -1 *n'en est pas un on a* $\left(\frac{p}{3}\right) = \begin{cases} 1, & \text{si } p \equiv 1 \pmod 3, \\ -1, & \text{si } p \equiv -1 \pmod 3, \end{cases}$ *et que* $\frac{p-1}{2} = \begin{cases} 1, & \text{si } p \equiv 1 \pmod 4, \\ -1, & \text{si } p \equiv -1 \pmod 4, \end{cases}$ *on en déduit que* $\left(\frac{3}{p}\right) = 1$ *si et seulement si*

$$p \equiv 1 \pmod 3 \text{ et } p \equiv 1 \pmod 4,$$

ou

$$p \equiv -1 \pmod 3 \text{ et } p \equiv -1 \pmod 4.$$

Puisque $3 \wedge 4 = 1$*, par le théorème chinois on a* $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}/12\mathbb{Z}$*, un isomorphisme étant donné par* $(a, b) \mapsto 4va + 3ub$*, où* $3u + 4v = 1$*. En prenant* $u = -1$ *et* $v = 1$*, on obtient que* 3 *est un carré modulo* p *si et seulement si*

$$p \equiv 4 - 3 \equiv 1 \pmod{12} \text{ ou } p \equiv -4 + 3 \equiv -1 \pmod{12}.$$

   (b) On suppose ici $p \neq 5$. Montrer que $\left(\frac{5}{p}\right) = p^2 \pmod 5$. *Par la loi de réciprocité quadratique on a* $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)(-1)^{\frac{(5-1)(p-1)}{4}} = \left(\frac{p}{5}\right)$ *puisque* p *est impair. On conclut puisque* $\left(\frac{p}{5}\right) = p^{\frac{5-1}{2}} = p^2 \pmod 5$*.*

2. L'entier 219 est-il un carré modulo 383 ? *Tout d'abord, on vérifie que* 383 *est premier, en divisant par tous les nombres premiers jusqu'à* 19 *(on a* $20^2 = 400 > 383$ *donc* $\sqrt{383} < 20$*). On a* $219 = 3 \times 73$ *donc* $\left(\frac{219}{383}\right) = \left(\frac{3}{383}\right)\left(\frac{73}{383}\right)$*. Par la loi de réciprocité quadratique on a*

$$\left(\frac{3}{383}\right) = (-1)^{\frac{2\times 282}{4}}\left(\frac{383}{3}\right) = -\left(\frac{-1}{3}\right) = 1,$$

et

$$\left(\frac{73}{383}\right) = (-1)^{\frac{72\times 282}{4}}\left(\frac{383}{73}\right) = \left(\frac{18}{73}\right).$$

Par suite, on a $18 = 2 \times 3^2$ *donc*

$$\left(\frac{73}{383}\right) = \left(\frac{18}{73}\right) = \left(\frac{2}{73}\right)\left(\frac{3}{73}\right)^2 = \left(\frac{2}{73}\right) = (-1)^{\frac{73^2-1}{8}} = 1,$$

car $73 \equiv 1 \pmod 8$*. Finalement, on a* $\left(\frac{3}{383}\right) = 1$ *donc* 219 *est un carré modulo* 383*.*

Exercice 13 (Perrin exo 4.13 p.93)**.** Soit p un nombre premier impair.

1. Montrer que $\sum_{x\in\mathbb{F}_p^\times}\left(\frac{x}{p}\right) = 0$. *En utilisant le morphisme* $\mathbb{F}_p^\times \to \mathbb{F}_p^\times$ *donné par* $x \mapsto x^2$*, on sait que* $\mathbb{F}_p^\times$ *contient autant de carrés que de non carrés, ce qui conclut.*
2. Soit $\zeta \in \mu_p^\times(\mathbb{C})$. On pose $s \coloneqq \sum_{x\in\mathbb{F}_p^\times}\left(\frac{x}{p}\right)\zeta^x$ (« somme de Gauss »).
   (a) Montrer que $s^2 = \sum_{x,y\in\mathbb{F}_p^\times}\left(\frac{y}{p}\right)\zeta^{x(1+y)}$. *On a* $s^2 = \sum_{x,y\in\mathbb{F}_p^\times}\left(\frac{xy}{p}\right)\zeta^{x+y} = \sum_{x,y\in\mathbb{F}_p^\times}\left(\frac{xy}{p}\right)\zeta^{x(1+x^{-1}y)}$ *donc puisque* $y \mapsto x^{-1}y$ *est une permutation de* $\mathbb{F}_p^\times$ *on obtient* $s^2 = \sum_{x,z\in\mathbb{F}_p^\times}\left(\frac{x^2z}{p}\right)\zeta^{x(1+z)}$*. Finalement, puisque le symbole de Legendre est un morphisme et que* $\left(\frac{x}{p}\right) = \pm 1$ *on obtient* $s^2 = \sum_{x,z\in\mathbb{F}_p^\times}\left(\frac{z}{p}\right)\zeta^{x(1+z)}$ *comme demandé.*
   (b) En séparant la somme précédente pour $y = -1$ et $y \neq -1$, montrer que $s^2 = \left(\frac{-1}{p}\right)p$. *Puisque* $\zeta^{1+y} \neq 1$ *si* $y \in \mathbb{F}_p$ *est différent de* -1 *(puisque*

$\zeta \in \mathbb{C}^\times$ *est d'ordre* p*) on obtient*

$$\begin{aligned}
s^2 &= \sum_{x\in\mathbb{F}_p^\times} \left(\frac{-1}{p}\right) + \sum_{\substack{x\in\mathbb{F}_p^\times \\ y\in\mathbb{F}_p^\times\setminus\{-1\}}} \left(\frac{y}{p}\right)\zeta^{x(1+y)} \\
&= \left(\frac{-1}{p}\right)(p-1) + \sum_{y\in\mathbb{F}_p^\times\setminus\{-1\}} \left(\frac{y}{p}\right)\sum_{x=1}^{p-1}(\zeta^{1+y})^x \\
&= \left(\frac{-1}{p}\right)(p-1) + \sum_{y\in\mathbb{F}_p^\times\setminus\{-1\}} \left(\frac{y}{p}\right)\zeta^{1+y}\frac{\zeta^{(1+y)(p-1)}-1}{\zeta^{1+y}-1} \\
&= \left(\frac{-1}{p}\right)(p-1) + \sum_{y\in\mathbb{F}_p^\times\setminus\{-1\}} \left(\frac{y}{p}\right)\zeta^{1+y}\frac{\zeta^{-(1+y)}-1}{\zeta^{1+y}-1} \\
&= \left(\frac{-1}{p}\right)(p-1) + \sum_{y\in\mathbb{F}_p^\times\setminus\{-1\}} \left(\frac{y}{p}\right)\frac{1-\zeta^{1+y}}{\zeta^{1+y}-1} \\
&= \left(\frac{-1}{p}\right)(p-1) - \sum_{y\in\mathbb{F}_p^\times\setminus\{-1\}} \left(\frac{y}{p}\right).
\end{aligned}$$

Ainsi, par la question 1 on obtient

$$s^2 = \left(\frac{-1}{p}\right)(p-1) + \left(\frac{-1}{p}\right) = \left(\frac{-1}{p}\right)p.$$

3. On veut montrer le cas particulier suivant du théorème de Kronecker–Weber : toute extension quadratique (c'est-à-dire de degré 2) de $\mathbb{Q}$ est une sous-extension d'une extension cyclotomique.
   (a) Rappeler pourquoi toute extention quadratique de $\mathbb{Q}$ est de la forme $\mathbb{Q}(\sqrt{d})$ avec $d \in \mathbb{Z}\setminus\{0,1\}$ sans facteur carré. *Soit* $K/\mathbb{Q}$ *une extention de degré* 2*. Si* $x \in K\setminus\mathbb{Q}$ *alors* $\mathbb{Q} \subsetneq \mathbb{Q}(x) \subseteq K$ *donc* $K = \mathbb{Q}(x)$ *par passage au degré (on a démontré un cas particulier du théorème de l'élément primitif). Ainsi, le polynôme minimal* π_x *de* x *sur* $\mathbb{Q}$ *est de degré* 2*. S'il est de la forme* X^2+b *c'est gagné (on peut se ramener au cas où* b *est sans facteur carré juste en multipliant : si* $b = c^2d$ *alors* $\sqrt{b} = c\sqrt{d}$ *donc* $\mathbb{Q}(\sqrt{b}) = \mathbb{Q}(\sqrt{d})$*). Sinon,* π_x *est de la forme* $X^2+2aX+b = (X+a)^2-a^2+b$ *donc on est ramené au cas précédent avec l'élément* $x-a$*, qui engendre également* K *sur* $\mathbb{Q}$*.*
   (b) Montrer que si $\zeta_n \in \mu_n^\times(\mathbb{C})$ pour tout $n \in \mathbb{N}^*$ alors $\mathbb{Q}(\zeta_m,\zeta_n) \subseteq \mathbb{Q}(\zeta_{m\vee n})$ pour tout $m,n \in \mathbb{N}^*$. *Indication* : on pourra utiliser la question 1 de l'Exercice 2. *Par l'indication* $\zeta_{m\vee n}^{\frac{n}{m\wedge n}} \in \mathbb{C}^\times$ *est d'ordre* m *donc* ζ_m *en est une puissance donc* $\zeta_m \subseteq \mathbb{Q}(\zeta_{m\vee n})$*. De même pour* ζ_n *donc* $\mathbb{Q}(\zeta_m,\zeta_n) \subseteq \mathbb{Q}(\zeta_{m\vee n})$*.*
   (c) Montrer qu'il suffit de se ramener au cas $d > 0$. *Soit* $d > 0$*. On a* $\mathbb{Q}(\sqrt{-d}) = \mathbb{Q}(i\sqrt{d}) \subseteq \mathbb{Q}(i,\sqrt{d})$*. Si le théorème est vrai pour* $d > 0$*, alors il existe une racine primitive* $\zeta \in \mathbb{C}^\times$ *tel que* $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\zeta)$*. Puisque* i *est une racine (primitive quatrième) de l'unité, on conclut par la question précédente.*

(d) Déduire des questions précédentes que l'on peut se ramener au cas d premier (positif). *Écrivons $d = p_1 \cdots p_r$ (rappelons que d est sans facteur carré). Si le théorème est vrai pour chaque p_i alors il existe des racines de l'unité $\zeta_1, \ldots, \zeta_r \in \mathbb{C}^\times$ tel que $\sqrt{p_k} \in \mathbb{Q}(\zeta_k)$ (attention, la notation est ambiguë : ζ_k n'est pas nécessairement une racine kième de l'unité). Par la question 3.(b) on a $\sqrt{d} = \sqrt{p_1} \cdots \sqrt{p_r} \in \mathbb{Q}(\zeta_1, \ldots, \zeta_r) \subseteq \mathbb{Q}(\zeta)$ pour une certaine racine de l'unité ζ.*

(e) Montrer le théorème dans le cas $d = 2$. *Soit $\zeta_8 := e^{\frac{i\pi}{4}} = (1+i)\frac{\sqrt{2}}{2} \in \mu_8^\times(\mathbb{C})$. On a $i = \zeta_8^2$ donc $\sqrt{2} \in \mathbb{Q}(\zeta_8)$, ce qui conclut.*

(f) Montrer le théorème. *Par ce qui précède, il suffit de montrer le théorème pour $d = p$ premier impair. Par la quesiton 2.(b), on sait que $\left(\frac{-1}{p}\right)$ p est un carré dans un $\mathbb{Q}(\zeta_p)$. Si $\left(\frac{-1}{p}\right) = 1$ on conclut, et sinon p est un carré dans $\mathbb{Q}(i, \zeta_p)$ donc on conclut par la question 3.(b).*