1 Corps finis

1.1 Problèmes

Soit p un nombre premier ; on s'intéresse à l'ensemble des carrés de $(\mathbb{Z}/p\mathbb{Z})^*$, c'est-à-dire le sous-ensemble des éléments de la forme x^2 avec $x \in (\mathbb{Z}/p\mathbb{Z})^*$. Comme la question est vite résolue pour p pair, on le suppose impair.

Si x est un entier premier à p, on pose $\left(\frac{x}{p}\right) = 1$ si la réduction modulo p de x est un carré de $(\mathbb{Z}/p\mathbb{Z})^*$: on dit alors que x est un résidu quadratique modulo p. On pose $\left(\frac{x}{p}\right) = -1$ si ce même x n'est pas un carré de $(\mathbb{Z}/p\mathbb{Z})^*$, et enfin $\left(\frac{x}{p}\right) = 0$ si p divise x ; on appelle symbole de Legendre l'application $\left(\frac{\cdot}{p}\right) : \mathbb{Z} \to \{1, 0, 1\}$ ainsi définie. L'objectif de cet exercice est d'établir quelques propriétés classiques du symbole de Legendre, notamment pour son calcul pratique, avec comme point culminant le théorème suivant :

Théorème 1 (Loi de réciprocité quadratique): Si p et q sont deux nombres impairs, alors :

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

Ainsi, par exemple, si p ou q est congru à 1 modulo 4, alors p est un résidu quadratique modulo q si, et seulement si q est un résidu quadratique modulo p.

Introduisons quelques notations standard : soit d un entier qui n'est pas un carré parfait. Si $d < 0$, on pose $\sqrt{d} = i\sqrt{|d|}$. On note alors $\mathbb{Q}(\sqrt{d})$ le plus petit corps contenant $\mathbb{Q}$ et $\sqrt{d}$; il contient exactement les nombres complexes de la forme $a + b\sqrt{d}$, avec a et b des nombres rationnels. Soit q un nombre premier impair. On note $\mathbb{Q}(\zeta_q)$ le plus petit corps contenant $\mathbb{Q}$ et un générateur ζ_q du groupe des racines q-ièmes de l'unité ; on peut vérifier qu'il contient exactement les nombres complexes de la forme $a_0 + a_1\zeta_q + \cdots + a_{q-2}\zeta_q^{q-2}$, où les a_i sont des nombres rationnels.

Enfin, si K est un corps, on note $\mathrm{Aut}(K)$ l'ensemble de ses automorphismes de corps, qui est un groupe pour la composition. Pour $f \in \mathrm{Aut}(K)$, l'ensemble des points fixes de f est un sous-corps de K, donc contient son sous-corps premier, qui est de la forme $\mathbb{Q}$ ou $\mathbb{Z}/p\mathbb{Z}$ selon les situations.

Prérequis :
- anneaux-quotients, idéaux premiers et idéaux maximaux ;
- définition d'une action de groupe, stabilisateur, formule des classes (question 8) ;
- corps finis.

1. Les résultats classiques (lien avec $x^{\frac{p-1}{2}}$ *etc.*).
2. Soit p un nombre premier impair qui ne divise pas d. Montrer que l'idéal (p) est premier dans l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$ si, et seulement si d n'est pas un résidu quadratique modulo p. Montrer que sinon, on a $(p) = \mathfrak{p}_1\mathfrak{p}_2$ où les deux idéaux du produit sont des idéaux premiers (Indication : si $A = \mathbb{Z}[\sqrt{d}]$, on écrira $A/(p)$ comme un quotient de l'anneau de $\mathbb{Z}/p\mathbb{Z}[X]$ par $X^2 - d$, et on étudiera l'irréductibilité de ce dernier).

   L'objectif des questions suivantes est de démontrer la loi de réciprocité quadratique.
3. Montrer que pour tout d entier non nul qui n'est pas un carré parfait, $\mathrm{Aut}(\mathbb{Q}(\sqrt{d}))$ est isomorphe à $\{-1, 1\}$.
4. Montrer que $G = \mathrm{Aut}(\mathbb{Q}(\zeta_q))$ est isomorphe à $(\mathbb{Z}/q\mathbb{Z})^*$.
5. Montrer que $q^* = (-1)^{\frac{q-1}{2}}q$ est un carré dans $\mathbb{Q}(\zeta_q)$ (donc $\mathbb{Q}(\sqrt{q^*})$ est un sous-corps de $\mathbb{Q}(\zeta_q)$). (Indication : on montrera que $q = \prod_{i=1}^{(q-1)/2}(-\zeta_q^{-i})(1-\zeta_q^i)^2)$
6. Montrer que les automorphismes de $\mathbb{Q}(\zeta_q)$ qui fixent L sont exactement les éléments du sous-groupe de G d'indice 2 isomorphe au sous-groupe des carrés de $(\mathbb{Z}/q\mathbb{Z})^*$; on note H ce sous-groupe de G.

7. Soit p un nombre premier impair, distinct de q, et soit $\mathfrak{p}$ un idéal premier de l'anneau des entiers de $\mathbb{Q}(\sqrt{q^*})$ contenant (p) ; ils ont fait l'objet de la question 2. Montrer que le quotient de cet anneau par $\mathfrak{p}$ est isomorphe à $\mathbb{F}_p$ ou $\mathbb{F}_{p^2}$. Notons k ce corps. Montrer que l'ensemble des automorphismes de corps de $\mathbb{Q}(\sqrt{d})$ qui laissent stable $\mathfrak{p}$ est isomorphe à $\mathrm{Aut}(k)$, *via* l'application $\sigma \mapsto \bar{\sigma}$, où $\bar{\sigma}(x)$ est la réduction modulo $\mathfrak{p}$ de $\sigma(x)$ pour tout $x \in k$.

   En particulier, le groupe $\mathrm{Aut}(k)$ admet un générateur privilégié, à savoir le morphisme de Frobenius $x \mapsto x^p$. Soit $\sigma_\mathfrak{p} \in \mathrm{Aut}(\mathbb{Q}(\sqrt{d})$ tel que son image par l'isomorphisme précédent soit le morphisme de Frobenius (il est unique). On a donc $\sigma_\mathfrak{p}(x) - x^p \in \mathfrak{p}$ pour tout x dans l'anneau des entiers de $\mathbb{Q}(\sqrt{q^*})$.
8. Soit $\mathfrak{P}$ un idéal premier de $\mathbb{Z}(\zeta_q)$ contenant $\mathfrak{p}$ (donc contenant (p)). Montrer que le quotient de cet anneau par $\mathfrak{P}$ est un corps fini. Notons k' ce corps. Montrer que l'ensemble des automorphismes de corps de $\mathbb{Q}(\zeta_q)$ qui laissent stable $\mathfrak{P}$ est isomorphe à $\mathrm{Aut}(k')$, *via* l'application de réduction modulo $\mathfrak{P}$, écrite ainsi : $\sigma \mapsto \bar{\sigma}$.
   En particulier, le groupe $\mathrm{Aut}(k')$ admet un générateur privilégié, à savoir le morphisme de Frobenius $x \mapsto x^p$. Soit $\sigma_\mathfrak{P} \in G$ tel que son image par l'isomorphisme précédent soit le morphisme de Frobenius (il est unique). On a donc $\sigma_\mathfrak{P}(x) - x^p \in \mathfrak{P}$ pour tout x dans $\mathbb{Z}[\zeta_q]$.
9. Montrer que $\sigma_\mathfrak{P}(\zeta_q) = \zeta_q^p$.
10. Justifier que la restriction de $\sigma_\mathfrak{P}$ à $\mathbb{Q}(\sqrt{q^*})$ est $\sigma_\mathfrak{p}$, et en déduire que si φ est l'isomorphisme entre $\mathrm{Aut}(\mathbb{Q}(\sqrt{q^*}))$ et $\{-1, 1\}$, alors $\varphi(\sigma_\mathfrak{p}) = \left(\frac{p}{q}\right)$.
11. Montrer que $\varphi(\sigma_\mathfrak{p}) = \left(\frac{q^*}{p}\right)$, et en comparant les relations obtenues, en déduire la loi de réciprocité quadratique.

1.2 Corrigé

1. (classique, à venir)
2. L'idéal (p) est premier si, et seulement si le quotient $A/\mathfrak{p}$, où A est l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$, est intègre. Si $A = \mathbb{Z}[\sqrt{d}]$ (cas où d est congru à 2 ou 3 modulo 4), alors

$$A/(p) \simeq (\mathbb{Z}[X]/(X^2 - d))/(p) \simeq \mathbb{Z}[X]/(X^2 - d, p) \simeq \mathbb{Z}/p\mathbb{Z}[X]/(X^2 - d).$$

   Ces isomorphismes d'anneaux méritent d'être détaillés au moins une fois : on a le diagramme suivant qui illustre les différents morphismes en présence,

$$\begin{array}{ccccc}
\mathbb{Z}/p\mathbb{Z}[X] \simeq \mathbb{Z}[X]/(p) & \xleftarrow{\pi_1} & \mathbb{Z}[X] & \xrightarrow{\pi_2} & \mathbb{Z}[X]/(X^2-d) \simeq \mathbb{Z}[\sqrt{d}]\ , \\
\downarrow{\scriptstyle \psi_1} & & \vdots & & \downarrow{\scriptstyle \psi_2} \\
(\mathbb{Z}/p\mathbb{Z}[X])/(X^2-d) & \longleftarrow & \mathbb{Z}[X]/\ker(\psi_1\circ\pi_1), \mathbb{Z}[X]/\ker(\psi_2\circ\pi_2) & \longrightarrow & (\mathbb{Z}[X]/(X^2-d))/(p)
\end{array}$$

   où toutes les flèches sont surjectives, et celles de la ligne du bas sont même des isomorphismes (à l'aide du théorème de factorisation de morphisme). Il suffit donc de montrer, pour avoir les isomorphismes désirés, l'égalité $\ker(\psi_1 \circ \pi_1) = \ker(\psi_2 \circ \pi_2)$. Je fais le calcul pour $\ker(\psi_1 \circ \pi_1)$, il suffira pour convaincre que ce n'est pas difficile, et qu'on trouve la même chose pour $\ker(\psi_2 \circ \pi_2)$.
   Soit $P \in \mathbb{Z}[X]$ tel que $\psi_1 \circ \pi_1(P) = 0$. Alors $\pi_1(P) \in \ker(\psi_1) = (X^2 - d)\mathbb{Z}/p\mathbb{Z}[X]$, donc $\pi_1(P) = (X^2 - d)\bar{Q}$ avec $\bar{Q} \in \mathbb{Z}/p\mathbb{Z}[X]$. Soit $Q \in \mathbb{Z}[X]$ tel que $\pi_1(Q) = \bar{Q}$, alors :

$$\pi_1(P - (X^2 - d)Q) = 0,$$

   donc $P - (X^2 - d)Q \in p\mathbb{Z}[X]$, et $P \in (X^2 - d)\mathbb{Z}[X] + p\mathbb{Z}[X] = (X^2 - d, p)$, c'est-à-dire $\ker(\psi_1 \circ \pi_1) \subseteq (X^2 - d, p)$. La réciproque est immédiate.

Bref, l'idéal (p) est premier si, et seulement si X^2-d est irréductible sur $\mathbb{Z}/p\mathbb{Z}$, si et seulement si ce même polynôme n'a pas de racine modulo p, si et seulement si d n'est pas un résidu quadratique modulo p. L'étude est la même si $A=\mathbb{Z}[\frac{1+d}{2}]$, car si $a+b\frac{1+\sqrt{d}}{2}$ est un élément de A, alors $a+(b+p)\frac{1+\sqrt{d}}{2}$ est un élément de $\mathbb{Z}[\sqrt{d}]$, et en fait $A/(p)\simeq\mathbb{Z}[\sqrt{d}]/(p)$.
Traitons le cas où d est congru à 2 ou 3 mod 4, l'autre cas étant analogue. Si $d\equiv a^2 \mod p$, alors les isomorphismes précédents montrent que $\mathfrak{p}_1=(p,a-\sqrt{d})$ est un idéal maximal (étant isomorphe à $\mathbb{Z}/p\mathbb{Z}[X]/(X-a)\simeq\mathbb{Z}/p\mathbb{Z}$), donc premier. De même, $\mathfrak{p}_2=(p,a+\sqrt{d})$ est un idéal maximal, et on doit maintenant prouver que le produit de ces deux idéaux égale (p). Soient $x=x_0p+x_1(a-\sqrt{d})\in\mathfrak{p}_1$ et $y=y_0p+y_1(a+\sqrt{d})\in\mathfrak{p}_2$. Comme a^2-d est dans (p), on a :

$$xy=x_0y_0p^2+p(x_0y_1(a+\sqrt{d})+x_1y_0(a-\sqrt{d}))+x_1y_1(a^2-d)\in(p),$$

donc $\mathfrak{p}_1\mathfrak{p}_2\subseteq(p)$ par stabilité de la somme dans les idéaux. En conséquence, le morphisme $\mathbb{Z}[\sqrt{d}]/\mathfrak{p}_1\mathfrak{p}_2\to\mathbb{Z}[\sqrt{d}]/(p)$ qui envoie $x \mod \mathfrak{p}_1\mathfrak{p}_2$ sur $x \mod (p)$ est bien défini et surjectif. Comme les cardinaux sont égaux en vertu des isomorphismes de la correction de la question 2 et de l'isomorphisme « du lemme chinois » $A/\mathfrak{p}_1\mathfrak{p}_2\simeq A/\mathfrak{p}_1\times A/\mathfrak{p}_2$ *, ce morphisme est bijectif, donc injectif, donc $x\equiv 0 \mod (p)$ implique $x\equiv 0 \mod \mathfrak{p}_1\mathfrak{p}_2$, ce qui donne précisément l'inclusion inverse puis l'égalité.

La preuve est exactement la même si l'anneau des entiers est $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, en remplaçant néanmoins $\mathfrak{p}_1$ et $\mathfrak{p}_2$ par $\left(p,a-\frac{\sqrt{d}+1}{2}\right)$ et $\left(p,a-\frac{-\sqrt{d}+1}{2}\right)$, où a est une racine de $X^2-X-\frac{d-1}{4}$ modulo p.

3. Un tel morphisme σ coïncide avec l'identité sur $\mathbb{Q}$, donc est déterminé par l'image de $\sqrt{d}$. Comme $\sigma(\sqrt{d})^2=\sigma(\sqrt{d}^2)=d$, on a $\sigma(\sqrt{d})\in\{-\sqrt{d},\sqrt{d}\}$. Chaque choix définit bien un automorphisme de $\mathbb{Q}(\sqrt{d})$, comme on le vérifie immédiatement. Donc $\mathrm{Aut}(\mathbb{Q}(\sqrt{d}))$ est un groupe à deux éléments, isomorphe à $\{-1,1\}$.
4. De même, on peut déterminer un automorphisme de $\mathbb{Q}(\zeta_q)$ avec l'image d'un seul élément, à savoir ζ_q. Soit $P=\sum_{k=0}^{q-1}X^k=\frac{X^q-1}{X-1}$. Ce polynôme annule ζ_q (c'est, en fait, son polynôme minimal), et les propriétés de morphisme de σ permettent d'écrire

$$P(\sigma(\zeta_q))=\sum_{k=0}^{q-1}\sigma(\zeta_q)^k=\sigma\left(\sum_{k=0}^{q-1}\zeta_q^k\right)=\sigma(0)=0,$$

donc $\sigma(\zeta_q)$ est une racine q-ième de l'unité différente de 1, d'après l'écriture de P ci-dessus. Chaque choix de racine q-ième de l'unité fournit un automorphisme de corps, comme on le vérifie presque immédiatement ; pour la surjectivité, si $\sigma(\zeta_q)=\zeta_q^l$, alors écrire une relation de Bézout de la forme $ul+vq=1$ permet d'avoir $\sigma(\zeta_q^u)=\zeta_q$. Notons σ_l l'automorphisme qui envoie ζ_q sur ζ_q^l (sa réciproque est donc $\sigma_{l^{-1} \mod p}$) ; il ne dépend que de la classe de l modulo q. On a prouvé l'existence d'un isomorphisme entre $(\mathbb{Z}/q\mathbb{Z})^*$ et $\mathrm{Aut}(\mathbb{Q}(\zeta_q))$ donné par $l\mapsto\sigma_l$ (l'injectivité est immédiate).
5. On sait que $X^q-1=(X-1)\cdot(X^{q-1}+\cdots+X+1)=\prod_{i=0}^{q-1}(X-\zeta_q^i)$. On déduit de ceci l'égalité

$$X^{q-1}+\cdots+X+1=\prod_{i=1}^{q-1}(X-\zeta_q^i),$$

et en posant $X=1$, on obtient

$$q=\prod_{i=1}^{q-1}(1-\zeta_q^i)=\prod_{i=1}^{(q-1)/2}(1-\zeta_q^i)(1-\zeta_q^{-i})=\prod_{i=1}^{(q-1)/2}(-\zeta_q^{-i})(1-\zeta_q^i)^2.$$

∗. Le noyau de cette application est $\mathfrak{p}_1\cap\mathfrak{p}_2/\mathfrak{p}_1\mathfrak{p}_2$, or $\mathfrak{p}_1\cap\mathfrak{p}_2=\mathfrak{p}_1\mathfrak{p}_2$. En effet, $\mathfrak{p}_1+\mathfrak{p}_2$ est un idéal contenant $\mathfrak{p}_1$. Par maximalité de ce dernier, on a $\mathfrak{p}_1+\mathfrak{p}_2=\mathfrak{p}_1$ ou $\mathfrak{p}_1+\mathfrak{p}_2=A$, et le premier cas est exclu parce que $\mathfrak{p}_2$ est différent de $\mathfrak{p}_1$. Alors, il existe $p_1\in\mathfrak{p}_1$ et $p_2\in\mathfrak{p}_2$ tels que $1=p_1+p_2$, et tout élément x de $\mathfrak{p}_1\cap\mathfrak{p}_2$ s'écrit alors $x=xp_1+xp_2\in\mathfrak{p}_1\mathfrak{p}_2$, d'où $\mathfrak{p}_1\cap\mathfrak{p}_2\subseteq\mathfrak{p}_1\mathfrak{p}_2$, et l'inclusion réciproque est immédiate. Ce raisonnement doit rappeler le cas plus classique des entiers premiers entre eux, traité avec la relation de Bézout.

Comme $\zeta_q = (\zeta_q^{(q+1)/2})^2$ est un carré dans $\mathbb{Q}(\zeta_q)$, on en déduit que

$$q^* = \left(\prod_{i=1}^{(q-1)/2} \zeta_q^{-i(q+1)/2}(1-\zeta_q^i) \right)^2$$

est un carré dans $\mathbb{Q}(\zeta_q)$.

6. Soit H' l'ensemble des automorphismes de $\mathbb{Q}(\zeta_q)$ qui fixent $\mathbb{Q}(\sqrt{q^*})$. Montrons d'abord que H est inclus dans H' **(à rédiger)**. Alors, H' est au plus d'indice 2, mais n'est pas d'indice 1, car ça signifierait que tous les automorphismes de G fixent $\mathbb{Q}(\sqrt{q}^*)$.
7. Comme p ne divise pas q, on est dans le contexte de la question 2. Remarque préliminaire : un idéal premier contenant (p) est forcément un des idéaux de la décomposition étudiée en 2. En effet, supposons que $(p) = \mathfrak{p}_1\mathfrak{p}_2 \subseteq \mathfrak{p}$ avec $\mathfrak{p}$ différent de $\mathfrak{p}_1$ et $\mathfrak{p}_2$. Ça signifie qu'on peut trouver $x_1 \in \mathfrak{p}_1$ qui n'est pas dans $\mathfrak{p}$, et de même $x_2 \in \mathfrak{p}_2$ qui n'est pas dans $\mathfrak{p}$. Pourtant, x_1x_2 est dans $\mathfrak{p}_1\mathfrak{p}_2 = (p) \subseteq \mathfrak{p}$, donc x_1 ou x_2 est dans $\mathfrak{p}$ parce que $\mathfrak{p}$ est premier : absurde. Ainsi, $\mathfrak{p}$ contient un de ces deux idéaux, et comme ils sont maximaux ceci impose l'égalité.

   Le quotient est un corps, parce qu'on a vu lors de la correction de la question 2 que $\mathfrak{p}$ est un idéal maximal ; cette même question montre que le cardinal du corps égale p^2 si (p) est premier (et alors $(p) = \mathfrak{p}$), p sinon. La maximalité aurait aussi pu découler du fait qu'on a vu que le quotient par $\mathfrak{p}$ est fini, et il est intègre, donc est un corps.
   Le morphisme $\sigma \mapsto \bar{\sigma}$ de l'énoncé, qu'on va appeler morphisme de réduction, est bien défini : si A désigne l'anneau des entiers de $\mathbb{Q}(\sqrt{q^*})$, alors le morphisme $A \xrightarrow{\sigma} A \to A/\mathfrak{p} = k$ se factorise *via* le noyau de cette application, qui est exactement $\sigma(\mathfrak{p})$. Si $\sigma(\mathfrak{p}) = \mathfrak{p}$, ceci induit bien un endomorphisme du corps k, injectif comme tout morphisme de corps qui se respecte, donc bijectif parce que k est fini ; c'est bien un automorphisme. Distinguons les deux cas qui se présentent :
   Si $k = \mathbb{F}_p$, on est dans le cas où $\mathfrak{p} \neq (p)$, et par ailleurs $\mathrm{Aut}(k)$ est réduit à l'identité, donc le morphisme est évidemment surjectif. Il est injectif parce que dans ce cas, où $(p) = \mathfrak{p}_1\mathfrak{p}_2$, l'écriture explicite de $\mathfrak{p}_1$ et $\mathfrak{p}_2$ montre que l'automorphisme non trivial de $\mathbb{Q}(\sqrt{q^*})$ les échange, donc seule l'identité appartient à la source du morphisme de réduction. C'est donc un isomorphisme (peu intéressant).
   Si $k = \mathbb{F}_{p^2}$, le morphisme de l'énoncé est injectif, parce qu'on vérifie aisément que si σ est le seul automorphisme non trivial de $\mathbb{Q}(\sqrt{q^*})$ (il laisse bien stable $\mathfrak{p} = (p)$), alors il échange $\sqrt{q^*}$ et $-\sqrt{q^*}$. Mais alors, comme $\sigma(\sqrt{q^*}) = -\sqrt{q^*} \not\equiv \sqrt{q^*} \mod (p)$ (sinon on aurait 2 ou $\sqrt{q^*}$ dans (p), et dans les deux cas ce n'est clairement pas vrai, par exemple en prenant la norme de ces éléments dans $\mathbb{Q}(\sqrt{q^*})$), seule l'identité est dans le noyau du morphisme de l'énoncé. Là encore, les cardinaux de $\mathrm{Aut}(k)$ et $\mathrm{Aut}(\mathbb{Q}(\sqrt{q^*}))$ coïncident, donc cette application est un isomorphisme.
8. On utilise le même argument que dans la question précédente pour démontrer que le quotient est un corps fini.
   Pour montrer que le morphisme de réduction est un isomorphisme, on aimerait imiter la résolution de la question précédente, mais on ne connait pas la décomposition de $p\mathbb{Z}[\zeta_q]$ dans $\mathbb{Z}[\zeta_q]$. En opérant exactement comme dans la question 2, on voit que si $X^{q-1} + X^{q-2} + \cdots + 1$ s'écrit, modulo p, comme produit des irréductibles P_i (ils sont tous à la puissance 1, parce que ce polynôme est facteur de $P = X^q - 1$ qui n'a que des racines simples modulo p, vu que $P' = qX^{q-1}$ est premier à P), on a

$$p\mathbb{Z}[\zeta_q] = (p, P_1(\zeta_q)) \cdots (p, P_m(\zeta_q)).$$

   Un phénomène sympathique est que tous ces polynômes ont même degré. Plus précisément, si p est d'ordre n dans $(\mathbb{Z}/q\mathbb{Z})^*$, et β une racine primitive q-ième de l'unité dans une extension de $\mathbb{Z}/p\mathbb{Z}$, alors les facteurs irréductibles P_i sont de la forme :

$$P_i = \prod_{k=0}^{n-1} (X - \beta^{p^k s}), s \in \mathbb{Z}/q\mathbb{Z}.$$

Admettons-le un instant (on a juste besoin de savoir qu'ils sont de même degré). Par le même argument que dans la résolution de la question 7, $\mathfrak{P}$ est un des idéaux $(p, P_i(\zeta_q))$. **(finir rédaction)**

Il reste à prouver ce qu'on a annoncé sur les polynômes P_i : un facteur de $X^{q-1}+X^{q-2}+\cdots+1$ est nécessairement de la forme $\prod_{s\in I}(X-\beta^s)$ avec I un sous-ensemble de $(\mathbb{Z}/q\mathbb{Z})^*$. Ce facteur est à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ si, et seulement si $Q^p = Q$ (grâce au morphisme de Frobenius), si et seulement si $Q(X^p) = Q(X)^p$ (parce que le morphisme de Frobenius est un morphisme), si et seulement si :

$$\prod_{s\in I}(X^p-\beta^s) = \prod_{s\in I}(X-\beta^s)^p = \prod_{s\in I}(X^p-\beta^{ps}).$$

Ainsi, on voit que I doit être stable par multiplication par p. Les plus petites parties de $(\mathbb{Z}/q\mathbb{Z})^*$ stables par multiplication par p sont évidemment celles de la forme $I = \{s, ps, \ldots, p^{n-1}s\}$, d'où le résultat sur les facteurs irréductibles P_i.

9. Si on note $\sigma_p \in G$ l'automorphisme qui envoie ζ_q sur ζ_q^p, alors $\sigma_p(\zeta_q) \equiv \zeta_q^p \equiv \sigma_{\mathfrak{P}}(\zeta_q) \mod \mathfrak{P}$. Comme ζ_q engendre $\mathbb{Z}[\zeta_q]$ (et donc $\zeta_q \mod \mathfrak{P}$ engendre $\mathbb{Z}[\zeta_q]/\mathfrak{P}$), on en déduit que $\bar{\sigma_p} = \bar{\sigma_{\mathfrak{P}}}$, et donc $\sigma_p = \sigma_{\mathfrak{P}}$.
10. On a $\sigma_{\mathfrak{P}}(\mathfrak{P}) = \mathfrak{P}$, donc $\sigma_{\mathfrak{P}}(\mathfrak{P} \cap \mathbb{Q}(\sqrt{q^*})) = \mathfrak{P} \cap \mathbb{Q}(\sqrt{q^*})$, or $\mathfrak{P} \cap \mathbb{Q}(\sqrt{q^*}) = \mathfrak{p}$: on vérifie que $A/(\mathfrak{P} \cap \mathbb{Q}(\sqrt{q^*}))$ s'injecte dans $A/\mathfrak{p}$ qui est intègre, donc $\mathfrak{P} \cap \mathbb{Q}(\sqrt{q^*})$ est premier non nul dans A ; comme $\mathfrak{p}$ est contenu dans cet idéal et est maximal, on en déduit l'égalité. De plus, on a évidemment $\sigma_{\mathfrak{P}}(x) \equiv x^p \mod \mathfrak{p}$ pour tout $x \in \mathbb{Z}[\zeta_q] \cap \mathbb{Q}(\sqrt{q^*}) = A$. Ainsi, $\sigma_{\mathfrak{P}}$ restreint à $\mathbb{Q}(\sqrt{q^*})$ induit le morphisme de Frobenius sur k, donc égale $\sigma_{\mathfrak{p}}$.

    Ce morphisme $\sigma_{\mathfrak{P}}$ est l'identité sur $\mathbb{Q}(\sqrt{q^*})$ s'il appartient à H (d'après la question 5), c'est-à-dire si l'image de σ par l'isomorphisme $\mathrm{Aut}(\mathbb{Q}(\zeta_q)) \simeq (\mathbb{Z}/q\mathbb{Z})^*$ explicité auparavant est un carré dans $(\mathbb{Z}/q\mathbb{Z})^*$. C'est l'unique automorphisme non trivial sinon. Comme cette image est p d'après la question précédente, on a $\varphi(\sigma_{\mathfrak{p}}) = \left(\frac{p}{q}\right)$.
11. La résolution de la question 7, par exemple (on peut le prouver directement), montre bien que $\sigma_{\mathfrak{p}}$ est trivial si, et seulement si $k = \mathbb{F}_p$, c'est-à-dire si, et seulement si (p) se décompose en un produit de deux idéaux premiers, si et seulement si q^* est un résidu quadratique modulo p. Ceci prouve que $\varphi(\sigma_{\mathfrak{p}}) = \left(\frac{q^*}{p}\right)$. Or $\left(\frac{q^*}{p}\right) = \left(\frac{(-1)^{\frac{q-1}{2}}}{p}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}}\left(\frac{q}{p}\right)$. On en déduit, en joignant ceci à la question précédente :

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

    D'où le théorème.