Université Aix-Marseille 2019–2020

Master 1 – Mathématiques & Applications
Algèbre & Géométrie

Devoir Surveillé 2
correction

Exercice 1.

1. Supposons par l'absurde qu'il existe un isomorphisme de corps $\varphi : \mathbb{C} \to \mathbb{R}$. Alors, $\varphi(0) = 0$ et $\varphi(1) = 1$ car φ est notamment un morphisme de groupes entre $(\mathbb{C}, +)$ et $(\mathbb{R}, +)$, ainsi qu'entre $(\mathbb{C}^*, \times)$ et $(\mathbb{R}^*, \times)$, et en préserve donc les éléments neutres. Dès lors, $\varphi(i)$ serait un réel vérifiant $\varphi(i)^2 + 1 = \varphi(i^2 + 1) = \varphi(0) = 0$, ce qui est absurde. Les corps $\mathbb{R}$ et $\mathbb{C}$ ne sont donc pas isomorphes.
2. Commençons par montrer que $\sqrt{\frac{7}{3}}$, $\sqrt{3}$ et $\sqrt{7}$ sont irrationnels. Supposons pour cela que $\sqrt{\frac{7}{3}} = \frac{p}{q}$ (resp. $\sqrt{3}$, $\sqrt{7}$) avec $p, q \in \mathbb{Z}^*$. On a alors $3p^2 = 7q^2$ (resp. $p^2 = 3q^2$, $p^2 = 7q^2$), ce qui est absurde car la valuation en 7 (resp. 3, 7) du terme de gauche est paire alors qu'elle est impaire pour le terme de droite.

   Supposons maintenant par l'absurde qu'il existe un isomorphisme de corps $\psi : \mathbb{Q}(\sqrt{7}) \to \mathbb{Q}(\sqrt{3})$. Par le même raisonnement qu'à la question précédente, on a alors $\psi(0) = 0$ et $\psi(1) = 1$, et de cela on peut déduire par récurrence que $\psi_{|\mathbb{Z}} = \mathrm{Id}_{\mathbb{Z}}$—en effet, on a alors $\psi(n) = \psi(n-1+1) = \psi(n-1)+1$—puis que $\psi_{|\mathbb{Q}} = \mathrm{Id}_{\mathbb{Q}}$—en effet, on a alors $\psi\left(\frac{p}{q}\right) = \psi(p)\psi\left(\frac{1}{q}\right)$ et $\psi\left(\frac{1}{q}\right) = \psi(q^{-1}) = \psi(q)^{-1} = \frac{1}{q}$.

   Par ailleurs, on a $\mathbb{Q}(\sqrt{3}) = \left\{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\right\}$. Le terme de droite est en effet un sous-corps de $\mathbb{R}$ puisqu'il est non vide—il contient 0—et stable par addition, multiplication—on a en effet $(a_1 + b_1\sqrt{3})(a_2 + b_2\sqrt{3}) = (a_1a_2 + 3b_2b_2) + (a_1b_2 + a_2b_1)\sqrt{3}$—et inverse—on a en effet $(a + b\sqrt{3})\left(\frac{a}{a^2-3b^2} - \frac{b}{a^2-3b^2}\sqrt{3}\right) = 1$ avec $a^2 - 3b^2 \neq 0$ car $\sqrt{3} \notin \mathbb{Q}$.

   Dès lors, on posant $\psi(\sqrt{7}) =: a + b\sqrt{3}$, on aurait $(a + b\sqrt{3})^2 = \psi(\sqrt{7}^2) = 7$, et donc $2ab\sqrt{3} = 7 - a^2 - 3b^2$. Par irrationalité de $\sqrt{3}$, on a donc $a = 0$ ou $b = 0$. Dans le premier cas, on aurait $3b^2 = 7$, contredisant l'irrationalité de $\sqrt{\frac{7}{3}}$. Dans le second cas, on aurait $a^2 = 7$, ce qui contredit l'irrationalité de $\sqrt{7}$.

   Dans tous les cas, on aboutit à une contradiction. les deux corps ne sont donc pas isomorphes.

Exercice 2.

1. (a) Le polynôme $X^n - 1$ est de degré n. Or sur un corps, un polynôme ne peut pas avoir plus de racines que son degré. On en déduit que $X^n - 1$ a au plus n racines.
   (b) i. Soit $x \in H$. D'après le théorème de Lagrange, $|x|$ divise $|H|$. Or par hypothèse $|H| = p^\alpha q$ avec $p \wedge q = 1$; on a donc $|x| = p^\beta q'$, avec $\beta \in [\![0, \alpha]\!]$ et q' divisant q. Si $|x|$ n'est pas divisible par p^α, alors on a même $\beta \in [\![0, \alpha - 1]\!]$ et donc $|x| = p^\beta q'$ divise $p^{\alpha-1}q = \frac{|H|}{p}$. Autrement dit, on a $\frac{|H|}{p} = k.|x|$ avec $k \in \mathbb{N}^*$.

   Dès lors, on a $x^{\frac{|H|}{p}} = x^{k.|x|} = \left(x^{|x|}\right)^k = 1^k = 1$ et x est racine de $X^{\frac{|H|}{p}} - 1$.
   ii. Supposons par l'absurde que tous les éléments de H ont un ordre non divisible par p, alors d'après la question précédente, cela donnerait $|H|$ racines au polynôme $X^{\frac{|H|}{p}} - 1$, lequel n'en possède qu'au plus $\frac{|H|}{p} < |H|$ d'après la question 1.(a). On en déduit qu'il existe au moins un élément dans H d'ordre divisible par p^α.
   iii. D'après la question précédente, il existe $x \in H$ d'ordre $p^\alpha q$ avec $q \in \mathbb{N}^*$. L'élément $x^q \in H$ est alors d'ordre p^α.
   (c) On commence par écrire $|H| = \prod_{i=1^r} p_i^{\alpha_i}$ avec $p_1, \ldots, p_r$ premiers deux à deux distincts et $\alpha_1, \ldots, \alpha_r \in \mathbb{N}^*$. D'après la question précédente, il existe $x_1, \ldots, x_r \in H$ tels que $|x_i| = p_i^{\alpha_i}$. Or, dans un groupe alébien, un produit d'éléments dont les ordres sont premiers entre eux a pour ordre le produit des ordres. On en déduit que $x_0 := x_1.\cdots.x_r \in H$ est d'ordre $\prod_{i=1^r} p_i^{\alpha_i} = |H|$ et donc que H est monogène.

2. D'après la question précédente, il existe un élément $x_0 \in \mathbb{F}_q^*$ d'ordre $|\mathbb{F}_q^*| = q-1$. Dès lors, $x_0^{\frac{q-1}{d}}$ est d'ordre d.

Exercice 3.

1. (a) Puisque $p \neq 2$, commençons par remarquer que, dans $\mathbb{F}_{p^2}$, $-1 \neq 1$.
   Si $\alpha \in \mathbb{F}_{p^2}$ est racine de P, alors $\alpha^4 = -1$. On en déduit que α n'est d'ordre ni 4, ni 2, ni 1, mais que $\alpha^8 = 1$, c'est-à-dire que $|\alpha|$ divise 8. L'ordre de α vaut donc 8.
   Réciproquement, si α est d'ordre 8, alors $(\alpha^4+1)(\alpha^4-1) = \alpha^8 - 1 = 0$. Par intégrité de $\mathbb{F}_{p^2}$, on a donc $\alpha^4 + 1 = 0$ ou $\alpha^4 - 1 = 0$, mais ce dernier cas n'est pas possible car sinon α serait d'ordre au plus 4. On en déduit donc que α est racine de P.
   (b) Soit $\alpha \in \mathbb{F}_{p^2}$ racine de P. Alors $(-\alpha)^4 + 1 = (\alpha)^4 + 1 = 0$, $\left(\alpha^{-1}\right)^4 + 1 = \frac{1+\alpha^4}{\alpha^4} = 0$ et $\left(-\alpha^{-1}\right)^4 + 1 = \left(\alpha^{-1}\right)^4 + 1 = 0$. Les éléments $-\alpha$, α^{-1} et $-\alpha^{-1}$ sont donc aussi racines de P.
   (c) Commençons par montrer que P possède une racine dans $\mathbb{F}_{p^2}$. D'après la question 1.(a), il suffit de montrer qu'il existe un élément d'ordre 8 dans $\mathbb{F}_{p^2}^*$; et pour cela, d'après la dernière question de l'exercice 2, il suffit de montrer que 8 divise $p^2 - 1$. Or, puisque p est impair, $p^2 - 1 = (p-1)(p+1)$ est un produit de deux nombres pairs consécutifs, et parmi deux nombres pairs consécutifs, l'un est nécessairement divisible par 4. On en conclut que $p^2 - 1$ est bien divisible par 8, et donc que P admet une racine α_0 dans $\mathbb{F}_{p^2}$.
   D'après la question 1.(b), les nombres $-\alpha_0$, α_0^{-1} et $-\alpha_0^{-1}$ sont aussi racines de P. Or ces quatres nombres sont distincts. En effet $\alpha_0 = -\alpha_0$ implique $\alpha_0 = 0$ puisque $p \neq 2$ or 0 n'est pas racine de P ; $\alpha_0 = \alpha_0^{-1}$ implique $\alpha_0^2 = 1$ or α_0 est d'ordre 8 ; $\alpha_0 = -\alpha_0^{-1}$ implique $\alpha_0^4 = 1$ or α_0 est d'ordre 8 ; et les trois derniers cas s'obtiennent enfin en remplaçant α_0 par $-\alpha_0$ ou α_0^{-1} dans ce qui précède. Le polynôme P, de degré 4, admet donc 4 racines distinctes, il est de fait scindé.
2. Montrons qu'il s'agit d'un sous-corps :
   - c'est un ensemble non vide car $1^p - 1 = 0$;
   - c'est stable par addition et opposé car, le morphisme de Frobénius étant linéaire sur $\mathbb{F}_{p^2}$, $(x_1+x_2)^p-(x_1+x_2) = x_1^p-x_1+x_2^p-x_2 = 0+0 = 0$ ainsi que $(-x)^p-(-x) = -(x^p-x) = -0 = 0$ pour x, x_1, x_2 racines de $X^p - X$;
   - c'est stable par multiplication et inverse car $(x_1x_2)^p-(x_1x_2) = x_1^px_2^p-x_1x_2 = x_1x_2-x_1x_2 = 0$ et $(x^{-1})^p - x^{-1} = (x^p)^{-1} - x^{-1} = x^{-1} - x^{-1} = 0$ pour x, x_1, x_2 racines de $X^p - X$.

   De plus, ce sous-corps contient au plus p éléments car $X^p - X$ ne peut pas possèder plus de p racines d'après la question 1.(a) de l'exercice 2. Or il contient $0, 1, 1+1 = 2, 2+1 = 3, \ldots, (p-2)+1 = p-1$. On en déduit qu'il s'agit d'un corps à p éléments, isomorphe à $\mathbb{Z}/p\mathbb{Z} =: \mathbb{F}_p$.
3. (a) On a $(\alpha+\alpha^{-1})^2 = \alpha^2 + 2 + \alpha^{-2}$, or $\alpha^4 + 1 = 0$ donc $\alpha^2 + \alpha^{-2} = 0$, d'où $(\alpha+\alpha^{-1})^2 = 2$.
   (b) i. Par division euclidienne, on a $k = 8k' + r$ avec $k' \in \mathbb{Z}$ et $r \in [\![0, 7]\!]$, et donc $\alpha^k = \left(\alpha^8\right)^{k'}.\alpha^r = \alpha^r$ d'après la question 1.(a).
   ii. Commençons par noter que, p étant impair, on a $p \equiv \pm 1$ ou $p \equiv \pm 3$ modulo 8.
   Par linéarité du morphisme de Frobenius, on a $(\alpha+\alpha^{-1})^p = \alpha^p + \alpha^{-p}$. D'après la question précédente, α^{-1} étant également racine de P, le résultat ne dépend que de la congruence de p modulo 8, avec :
   - si $p \equiv \pm 1 \mod 8$, $\alpha^p + \alpha^{-p} = \alpha^{\pm 1} + \alpha^{\mp 1}$;
   - si $p \equiv \pm 3 \mod 8$, $\alpha^p + \alpha^{-p} = \alpha^{\pm 3} + \alpha^{\mp 3} = -\alpha^{\mp 1} - \alpha^{\pm 1}$ puisque $\alpha^4 = -1$ et donc $\alpha^3 = -\alpha^{-1}$.

   On en déduit que $(\alpha+\alpha^{-1})^p = \varepsilon(\alpha+\alpha^{-1})$ avec $\varepsilon = 1$ si $p \equiv \pm 1 \mod 8$ et $\varepsilon = -1$ si $p \equiv \pm 3 \mod 8$.
   (c) D'après la question 2., un élément $x \in \mathbb{F}_{p^2}$ est dans $\mathbb{F}_p$ si et seulement si $x^p = x$, et d'après la question 3.(b).ii., $(\alpha+\alpha^{-1})^p = \alpha + \alpha^{-1}$ si et seulement si $p \equiv \pm 1 \mod 8$. On en déduit que $\alpha + \alpha^{-1} \in \mathbb{F}_p$ si et seulement si $p \equiv \pm 1 \mod 8$.
4. D'après la question 1.(c), il existe un racine α_0 de $X^4 + 1$ dans $\mathbb{F}_{p^2}$ et d'après la question 3.(a), on a $(\pm\alpha_0 + \pm\alpha_0^{-1})^2 = 2$. Or $X^2 - 2$ est de degré 2 et ne peut donc posséder qu'au plus 2 racines, à savoir $\pm(\alpha_0 + \alpha_0^{-1})$. La question est donc de savoir si ces deux racines sont dans $\mathbb{F}_p$ ou non. Or d'après la question 3.(c), elles le sont si et seulement si $p \equiv \pm 1 \mod 8$.

5. Pour $p = 3$, on a $p \equiv 3 \mod 8$ et, en effet, $\mathbb{F}_3$ ne possède pas de racine de 2 puisque $0^2 = 0$, $1^2 = 1$ et $2^2 = 1$.

   Pour $p = 7$, on $p \equiv -1 \mod 8$ et, en effet, $3^2 = 2$.

Exercice 4.

Une matrice de $\mathcal{M}_n(\mathbb{F}_p)$ est inversible si et seulement si ses colonnes forment une famille libre. Pour dénombrer $\mathrm{GL}_n(\mathbb{F}_p)$, il suffit donc de dénombrer le nombre de choix successivement possible pour chaque colonne.

- Pour la première colonne, il y a $p^n - 1$ possibilités, à savoir tous les vecteurs de taille n à valeurs dans $\mathbb{F}_p$ sauf le vecteur nul.
- Pour la seconde colonne, la première étant fixée, il y a $p^n - p$ possibilités, à savoir tous les vecteurs de taille n à valeurs dans $\mathbb{F}_p$ sauf les vecteurs colinéaires à la première colonne.
- Pour la troisième colonne, les deux premières étant fixée, il y a $p^n - p^2$ possibilités, à savoir tous les vecteurs de taille n à valeurs dans $\mathbb{F}_p$ sauf les vecteurs engendrés par les deux premières colonnes.
- Plus généralement, pour la $i^{\text{ième}}$ colonne, les $(i-1)$ premières étant fixée, il y a $p^n - p^{i-1}$ possibilités, à savoir tous les vecteurs de taille n à valeurs dans $\mathbb{F}_p$ sauf les vecteurs engendrés par les $(i-1)$ premières colonnes.

Au final, on a donc

$$\begin{aligned}
\left|\mathrm{GL}_n(\mathbb{F}_p)\right| &= \prod_{i=1}^{n}(p^n - p^{i-1}) \;=\; \prod_{i=1}^{n} p^{i-1}(p^{n-i+1} - 1) \\
&= \prod_{i=1}^{n} p^{i-1} \prod_{i=1}^{n}(p^{n-i+1} - 1) \;=\; p^{\sum_{i=1}^{n-1} i} \prod_{i=1}^{n}(p^i - 1) \\
&= p^{\frac{p(p-1)}{2}} \prod_{i=1}^{n}(p^i - 1).
\end{aligned}$$