

Exercice 1.

Soit $n > 0$ un entier positif. Montrez que $\cos(2\pi/n)$ et $\sin(2\pi/n)$ sont des nombres algébriques sur \mathbb{Q} .

Solution.

Comme (formules de partie réelles et imaginaires d'un nombre complexe)

$$\cos(2\pi/n) = \frac{e^{2\pi i/n} + ie^{-2\pi i/n}}{2} \quad \sin(2\pi/n) = \frac{e^{2\pi i/n} - e^{-2\pi i/n}}{2i}$$

on voit que $\cos(2\pi/n), \sin(2\pi/n) \in \mathbb{Q}(i, e^{2\pi i/n})$, ce qui conclut.

Exercice 2.

Soit $\alpha \in \mathbb{F}_{27}^\times$ un élément différent de 1 et -1 . Montrer que soit α , soit $-\alpha$, est un générateur du groupe cyclique \mathbb{F}_{27}^\times .

Solution.

Comme $26 = 13 * 2$ l'ordre multiplicatif d'un élément est 1, 2, 13 ou 26. Comme $\alpha \neq 1, -1$ et que ces éléments sont les seuls d'ordre 1 et 2 respectivement, l'ordre de α est 13 ou 26. Si α est d'ordre 26, c'est un générateur. S'il est d'ordre 13, alors $(-\alpha)^{13} = -1$. Il suit que $-\alpha$ est d'ordre 26.

Exercice 3.

Fixons un nombre premier p .

1. Pour $r > 0$, énumérez les sous-corps de \mathbb{F}_{p^r} . Si s divise r , énumérez les corps intermédiaires $\mathbb{F}_{p^s} \subseteq L \subseteq \mathbb{F}_{p^r}$.
2. Montrez que l'ensemble $\{0 \neq a \in \mathbb{F}_{16} \mid \mathbb{F}_2(a) = \mathbb{F}_{16} \text{ et } \langle a \rangle \neq \mathbb{F}_{16}^\times\}$ possède 4 éléments. Ici $\langle a \rangle$ désigne le sous-groupe de \mathbb{F}_{16}^\times généré par l'élément $a \neq 0$.
Indication : Etudiez la structure du groupe \mathbb{F}_{16}^\times .
3. Plus généralement, montrez que l'ensemble $\{0 \neq a \in \mathbb{F}_{p^4} \mid \mathbb{F}_p(a) = \mathbb{F}_{p^4} \text{ et } \langle a \rangle \neq \mathbb{F}_{p^4}^\times\}$ possède $p^4 - p^2 - \varphi(p^4 - 1)$ éléments, où φ est la fonction de comptage d'Euler.

Solution.

1. Par le Corollaire 4.4.22, \mathbb{F}_{p^r} contient un et un seul sous-corps isomorphe à \mathbb{F}_{p^n} pour n divisant r . Si \mathbb{F}_{p^s} est l'un d'eux, alors les corps intermédiaires de l'extension $\mathbb{F}_{p^s} \subset \mathbb{F}_{p^r}$ sont les \mathbb{F}_{p^n} où s divise n et n divise r .
2. Les sous-corps de \mathbb{F}_{16} , en vertu du premier point, sont \mathbb{F}_2 et \mathbb{F}_4 , et ils forment une chaîne. Donc $\mathbb{F}_2(a) = \mathbb{F}_{16}$ si et seulement si $a \notin \mathbb{F}_4$. Par le Théorème 4.2.17 on a

$$\mathbb{F}_{16}^\times \cong \mathbb{Z}/15\mathbb{Z}, \quad \mathbb{F}_4^\times \cong \mathbb{Z}/3\mathbb{Z}$$

et $\mathbb{F}_4^\times \subset \mathbb{F}_{16}^\times$ est un sous-groupe. Un élément $0 \neq a \in \mathbb{F}_{16}$ vérifie $\mathbb{F}_2(a) = \mathbb{F}_{16}$ si et seulement si son image dans \mathbb{F}_{16}^\times n'est pas contenue dans ce sous-groupe. D'un autre côté, il y a $\varphi(15) = 8$ éléments qui génèrent \mathbb{F}_{16}^\times , où φ est la fonction de comptage d'Euler. Remarquons aussi qu'un élément contenu dans le sous-groupe \mathbb{F}_4^\times ne saurait générer le groupe \mathbb{F}_{16}^\times . Il y a ainsi

$$|\mathbb{F}_{16}^\times| - |\mathbb{F}_4^\times| - \varphi(15) = 15 - 3 - 8 = 4$$

éléments $0 \neq a \in \mathbb{F}_{16}$ tels que $\mathbb{F}_2(a) = \mathbb{F}_{16}$ et $\langle a \rangle \neq \mathbb{F}_{16}^\times$.

3. L'argument est semblable à celui du point précédent. Les sous-corps de \mathbb{F}_{p^4} sont $\mathbb{F}_p \subset \mathbb{F}_{p^2}$, et on a $\mathbb{F}_p(a) = \mathbb{F}_{p^4}$ si et seulement si $a \notin \mathbb{F}_{p^2}$. Par le Théorème 4.2.17 on a

$$\mathbb{F}_{p^4}^\times \cong \mathbb{Z}/(p^4 - 1)\mathbb{Z}, \quad \mathbb{F}_{p^2}^\times \cong \mathbb{Z}/(p^2 - 1)\mathbb{Z}.$$

Notons $E := \{0 \neq a \in \mathbb{F}_{16} \mid \langle a \rangle = \mathbb{F}_{16}^\times\}$. Alors $|E| = \varphi(p^4 - 1)$. Remarquons aussi que E et $\mathbb{F}_{p^2}^\times$ sont des sous-ensembles disjoints de $\mathbb{F}_{p^4}^\times$. Ainsi

$$\begin{aligned} |\{0 \neq a \in \mathbb{F}_{p^4} \mid \mathbb{F}_p(a) = \mathbb{F}_{p^4} \text{ et } \langle a \rangle \neq \mathbb{F}_{p^4}^\times\}| &= |\mathbb{Z}/(p^4 - 1)\mathbb{Z} \setminus (E \sqcup \mathbb{F}_{p^2}^\times)| \\ &= p^4 - 1 - (p^2 - 1) - \varphi(p^4 - 1) \\ &= p^4 - p^2 - \varphi(p^4 - 1). \end{aligned}$$

Exercice 4 (Corps de décomposition sur \mathbb{F}_p).

Fixons un nombre premier $p > 0$ et un polynôme $f(x) \in \mathbb{F}_p[x]$ irréductible de degré d .

- Montrez que f divise $x^{p^d} - x$ dans $\mathbb{F}_p[x]$.
Indication : A l'aide du Théorème fondamental des corps finis, montrez que \mathbb{F}_{p^d} contient une racine de f .
- Montrez que $f(x)$ se scinde sur \mathbb{F}_{p^d} .
- Montrez que f n'a pas de racines multiples.
- Soit $g \in \mathbb{F}_p[x]$ un polynôme irréductible de degré d qui n'est pas associé à f . Montrez que f et g n'ont pas de racines en commun.
- Montrez que

$$x^{p^d} - x = \prod_{\substack{h \text{ unitaire irréd.} \\ \text{dans } \mathbb{F}_p[x] \\ \text{deg } h \text{ divise } d}} h.$$

Solution.

- Comme $\mathbb{F}_p[x]/(f)$ est un corps de cardinal p^d , on sait qu'il est isomorphe à \mathbb{F}_{p^d} par le théorème de classification des corps finis. Mais alors, il suit que f a une racine $\alpha \in \mathbb{F}_{p^d}$. Dès lors, on peut supposer quitte à rendre $f(x)$ unitaire que $m_\alpha(x) = f(x)$ car $f(x)$ est supposé irréductible. Mais comme $\alpha^{p^d} = \alpha$ car $\alpha \in \mathbb{F}_{p^d}$, on obtient donc $f(x) = m_\alpha(x) \mid x^{p^d} - x$, concluant.
- Le Théorème fondamental des corps finis nous indique que $x^{p^d} - x$ se scinde sur \mathbb{F}_{p^d} . Or f divise $x^{p^d} - x$, donc (par unicité de la décomposition en facteurs premiers) le polynôme f se scinde sur \mathbb{F}_{p^d} .
- Puisque f se scinde sur \mathbb{F}_{p^d} et divise $x^{p^d} - x$ dans $\mathbb{F}_{p^d}[x]$, il suffit de montrer que $x^{p^d} - x$ n'a pas de racines multiples dans \mathbb{F}_{p^d} . Or le Théorème fondamental des corps finis implique que

$$x^{p^d} - x \text{ est divisible par } \prod_{\alpha \in \mathbb{F}_{p^d}} (x - \alpha) \text{ dans } \mathbb{F}_{p^d}[x].$$

En comparant les degrés et les coefficients dominants, on voit qu'il y a en fait égalité entre ces deux polynômes. Donc $x^{p^d} - x$ n'a pas de racine multiple.

- Si par l'absurde α est une racine commune, alors $m_\alpha(x)$ divise tant bien f que g . Par suite, comme ces polynômes sont supposés irréductibles, on voit que ceux-ci sont associés.

5. Le premier point montre que $x^{p^d} - x$ est divisible par tous les polynômes irréductibles de degré d . La preuve du Corollaire 4.4.22 montre que $x^{p^s} - x$ divise $x^{p^d} - x$ pour tous les s divisant d . Donc

$$\prod_{\substack{h \text{ unitaire irréd.} \\ \text{dans } \mathbb{F}_p[x] \\ \deg h \text{ divise } d}} h \text{ divise } x^{p^d} - x.$$

Il reste à montrer qu'il n'existe pas d'autre polynôme irréductible divisant $x^{p^d} - x$. Soit g un polynôme irréductible dont le degré ne divise pas d . Si g divise $x^{p^d} - x$, alors g se scinde sur \mathbb{F}_{p^d} , et donc $\mathbb{F}_p[x]/(g)$ s'identifie à un sous-corps de \mathbb{F}_{p^d} , c'est-à-dire à un \mathbb{F}_{p^s} où s divise d . Mais dans ce cas

$$\deg g = [\mathbb{F}_p[x]/(g) : \mathbb{F}_p] = [\mathbb{F}_{p^s} : \mathbb{F}_p] = s$$

divise d , ce qui est une contradiction. On a donc l'égalité désirée.

Exercice 5.

Soit $f(t) \in \mathbb{F}_p[t]$ un polynôme de degré n . Montrez que $f(t)$ est irréductible si et seulement si $f(t)$ n'a pas de racines dans \mathbb{F}_{p^k} pour tout $1 \leq k \leq \lfloor \frac{n}{2} \rfloor$.

Une application de ce principe permet de montrer que $t^4 + 2 \in \mathbb{F}_5[t]$ est irréductible (voir Série 7.2.(b)). En effet, montrez qu'une racine α de ce polynôme a pour ordre multiplicatif* 16, mais que cela n'est pas possible pour des éléments de \mathbb{F}_{25} .

Solution.

Si $f(t)$ n'est pas irréductible alors il existe $g(t)$ irréductible de degré $k \leq \lfloor n/2 \rfloor$ qui divise $f(t)$. Or, $g(t)$ a une racine sur \mathbb{F}_{p^k} car

$$\mathbb{F}_p[t]/(g(t)) \cong \mathbb{F}_{p^k}.$$

Réciproquement si $f(t)$ a une racine α dans \mathbb{F}_{p^k} pour $k \leq \lfloor n/2 \rfloor < n$, alors $m_\alpha(t)$ le polynôme minimal de α divise f , mais $m_\alpha(t)$ est degré inférieur ou égal à k car $\mathbb{F}_p(\alpha) \subset \mathbb{F}_{p^k}$. Ainsi on a trouvé un polynôme non-constant de degré strictement inférieur à n divisant f , ce qui montre que f n'est pas irréductible.

Une racine de $t^4 + 2$ dans $\mathbb{F}_5[t]$ satisfait $\alpha^4 = 3$. Cependant, l'ordre multiplicatif de 3 dans \mathbb{F}_5 est 4, donc il suit que l'ordre multiplicatif de α est 16. Mais comme 16 ne divise pas 24, on voit que α ne peut être un élément de \mathbb{F}_{25} .

Exercice 6 (Polynômes irréductibles sur \mathbb{F}_p).

Fixons un nombre premier $p > 0$. Nous allons calculer le nombre N_d de polynômes irréductibles unitaires d'un degré fixé sur \mathbb{F}_p . (Rappelons qu'un polynôme est unitaire si son coefficient dominant vaut 1).

1. Montrez que

$$d \cdot N_d = \left| \mathbb{F}_{p^d} \setminus \bigcup_{L \subsetneq \mathbb{F}_{p^d}} L \right|$$

où L parcourt l'ensemble des sous-corps strictement inclus dans \mathbb{F}_{p^d} .

Indication : Utilisez les résultats de l'Exercice 4 et le Théorème fondamental des corps finis.

2. Montrez que

$$N_2 = \frac{p^2 - p}{2}, \quad N_3 = \frac{p^3 - p}{3}, \quad N_4 = \frac{p^4 - p^2}{4}, \quad N_5 = \frac{p^5 - p}{5}, \quad N_6 = \frac{p^6 - p^3 - p^2 + p}{6}.$$

*Plus petit entier n tel que $\alpha^n = 1$.

Pour établir une formule générale, il sera utile d'introduire la **fonction de Möbius**. Il s'agit de la fonction

$$\mu: \mathbb{N}_{>0} \longrightarrow \{-1, 0, 1\}$$

définie par

$$\mu(n) = \begin{cases} 0 & \text{si } n \text{ est divisible par } p^2 \text{ pour un premier } p, \\ 1 & \text{si } n = 1 \text{ ou si } n \text{ est le produit d'un nombre pair de premiers distincts,} \\ -1 & \text{si } n \text{ est le produit d'un nombre impair de premiers distincts.} \end{cases}$$

Ceci étant, passons au cas général :

3. Si n, m divisent d et sont premiers entre eux, montrez que $\mathbb{F}_{p^{d/n}} \cap \mathbb{F}_{p^{d/m}} = \mathbb{F}_{p^{d/nm}}$ dans \mathbb{F}_{p^d} .

4. Montrez que

$$N_d = \frac{1}{d} \sum_{r|d} \mu\left(\frac{d}{r}\right) p^r.$$

Indication : Soit $d = s_1^{i_1} \cdots s_n^{i_n}$ la décomposition en produit de nombres premiers. Montrez d'abord que

$$dN_d = \left| \mathbb{F}_{p^d} \setminus \bigcup_{j=1}^n \mathbb{F}_{p^{d/s_j}} \right|$$

puis développez le terme de droite grâce à la formule d'inclusion-exclusion.

Solution. Cette solution est adaptée de l'article *Counting Irreducible Polynomials over Finite Fields Using the Inclusion-Exclusion Principle* de S.K.Chebolu et J. Minác, dans *Math. Mag.* **84** (2011) 369-371.

1. On a vu dans l'Exercice 3 que tout polynôme f irréductible de degré d se scinde sur \mathbb{F}_{p^d} . On a vu dans le même exercice que f n'a pas de racines doubles, et que deux polynômes unitaires irréductibles de même degré n'ont pas de racines en commun. Si f_1, \dots, f_{N_d} sont les polynômes unitaires irréductibles de degré d et $R_{f_i} \subset \mathbb{F}_{p^d}$ les ensembles de racines, on a donc montré que

$$|R_{f_i}| = d \quad \text{et} \quad R_{f_i} \cap R_{f_j} = \emptyset \text{ si } i \neq j.$$

Ainsi on obtient

$$dN_d = |R_{f_1} \sqcup \cdots \sqcup R_{f_{N_d}}|.$$

Il reste à déterminer quels éléments de \mathbb{F}_{p^d} sont des racines de polynômes irréductibles de degré d . Remarquons que si $a \in \mathbb{F}_{p^d}$ est une racine de f_i , alors

$$\mathbb{F}_p(a) \cong \mathbb{F}_p[t]/(f_i(t))$$

et en prenant les degrés sur \mathbb{F}_p on obtient $[\mathbb{F}_p(a) : \mathbb{F}_p] = d$. Donc $\mathbb{F}_p(a) = \mathbb{F}_{p^d}$. Ainsi si a est une racine de f_i , il n'appartient à aucun sous-corps strict $L \subsetneq \mathbb{F}_{p^d}$. Inversément, supposons que $a \in \mathbb{F}_{p^d}$ n'appartienne à aucun sous-corps strict. Par le Théorème 4.2.17, a est racine de $x^{p^d} - x \in \mathbb{F}_p[x]$, donc de l'un de ses facteurs irréductibles de degré e . Alors $[\mathbb{F}_p(a) : \mathbb{F}_p] = e$, et si $e < d$ on obtient $\mathbb{F}_p(a) \subsetneq \mathbb{F}_{p^d}$, ce qui est une contradiction avec le choix de a . En définitive nous avons montré que

$$R_{f_1} \sqcup \cdots \sqcup R_{f_{N_d}} = \mathbb{F}_{p^d} \setminus \bigcup_{L \subsetneq \mathbb{F}_{p^d}} L$$

où L parcourt les sous-corps stricts de \mathbb{F}_{p^d} .

2. Le problème pour tirer une formule générale du point précédent est que les sous-corps L ne sont pas tous inclus les uns dans les autres, et que leurs intersections sont non-triviales. Pour les petites valeurs de d , il est cependant facile de passer en revue les sous-corps et leurs intersections. Nous utilisons sans plus y faire référence le Corollaire 4.4.22.

(a) $d = 2$. Le seul sous-corps strict de \mathbb{F}_{p^2} est \mathbb{F}_p . Donc

$$N_2 = \frac{p^2 - p}{2}.$$

(b) $d = 3$. Le seul sous-corps strict de \mathbb{F}_{p^3} est \mathbb{F}_p . Donc

$$N_3 = \frac{p^3 - p}{3}.$$

(c) $d = 4$. Les sous-corps stricts de \mathbb{F}_{p^4} sont $\mathbb{F}_p \subset \mathbb{F}_{p^2}$. Donc

$$N_4 = \frac{p^4 - p^2}{4}.$$

(d) $d = 5$. Le seul sous-corps strict de \mathbb{F}_{p^5} est \mathbb{F}_p . Donc

$$N_5 = \frac{p^5 - p}{5}.$$

(e) $d = 6$. Le premier cas non-trivial. Les sous-corps stricts sont

$$\mathbb{F}_{p^2} \supset \mathbb{F}_p \subset \mathbb{F}_{p^3}.$$

Ainsi

$$|\mathbb{F}_{p^6} \setminus (\mathbb{F}_{p^2} \cup \mathbb{F}_{p^3})| = |\mathbb{F}_{p^6}| - |\mathbb{F}_{p^2}| - |\mathbb{F}_{p^3}| + |\mathbb{F}_{p^2} \cap \mathbb{F}_{p^3}|.$$

L'intersection $\mathbb{F}_{p^2} \cap \mathbb{F}_{p^3}$ est un corps fini de caractéristique p , donc un corps de la forme \mathbb{F}_{p^s} où s divise à la fois 2 et 3. Donc $s = 1$ et le cardinal de l'intersection vaut p . Il s'ensuit que

$$N_6 = \frac{p^6 - p^3 - p^2 + p}{6}.$$

3. Observez que le Corollaire 4.4.22 permet d'écrire explicitement le réseau de sous-corps de n'importe quel corps fini. Puisque $\mathbb{F}_{p^{d/n}} \cap \mathbb{F}_{p^{d/m}}$ est un sous-corps à la fois de $\mathbb{F}_{p^{d/n}}$, de $\mathbb{F}_{p^{d/m}}$ et de \mathbb{F}_{p^d} , on utilise le Corollaire 4.4.22 pour identifier cette intersection. Elle est donnée par \mathbb{F}_{p^s} , où s est le plus grand entier qui divise à la fois d/n et d/m . Puisque n et m sont premiers entre eux, en considérant la décomposition de d en facteurs premiers on voit que $s = d/nm$.

4. Passons au cas général. Dans la formule établie au premier point, on peut évidemment prendre l'union sur l'ensemble des sous-corps stricts L qui sont maximaux. Par le Corollaire 4.4.22, ces sous-corps sont donnés par

$$F_j := \mathbb{F}_{p^{d/s_j}} \quad \text{avec } d = \prod_{j=1}^n s_j^{i_j} \text{ la décomposition en nombres premiers.}$$

Ecrivons $F_{j_1 \dots j_r} := F_{i_1} \cap \dots \cap F_{j_r}$. En utilisant le point précédent par induction sur t , on voit que $|F_{j_1 \dots j_t}| = p^{d/s_{j_1} \dots s_{j_t}}$. La formule d'inclusion-exclusion nous donne alors

$$\begin{aligned}
 dN_d &= |\mathbb{F}_{p^d}| - \left| \bigcup_{j=1}^n F_j \right| \\
 &= p^d - \sum_{t=1}^n (-1)^{t+1} \sum_{j_1 < \dots < j_t} |F_{j_1 \dots j_t}| \\
 &= p^d - \sum_{t=1}^n (-1)^{t+1} \sum_{j_1 < \dots < j_t} p^{d/s_{j_1} \dots s_{j_t}} \\
 &= \sum_{t=0}^n (-1)^t \sum_{j_1 < \dots < j_t} p^{d/s_{j_1} \dots s_{j_t}}
 \end{aligned}$$

où on pose $p^{d/s_{j_1} \dots s_{j_t}} = p^d$ pour $t = 0$. Considérons maintenant un entier r divisant d . On a

$$r = \prod_{j=1}^n s_j^{k_j} \quad \text{avec } 0 \leq k_j \leq i_j, \quad \text{donc } \frac{d}{r} = \prod_{j=1}^n s_j^{i_j - k_j}.$$

Par la définition de la fonction de Möbius, on obtient

$$\mu\left(\frac{d}{r}\right) = \begin{cases} 0 & \text{si } k_j \leq i_j - 2 \text{ pour au moins un } j, \\ 1 & \text{si } \forall j : k_j \geq i_j - 1 \text{ avec égalité pour un nombre pair de } j, \\ -1 & \text{si } \forall j : k_j \geq i_j - 1 \text{ avec égalité pour un nombre impair de } j. \end{cases}$$

Il s'ensuit que

$$\sum_{t=0}^n (-1)^t \sum_{j_1 < \dots < j_t} p^{d/s_{j_1} \dots s_{j_t}} = \sum_{r|d} \mu\left(\frac{d}{r}\right) p^r$$

ce qui conclut l'exercice.