TD 11 : corrigé

1. Groupe additif d'un corps fini

Si K est un corps de cardinal $q = p^n$ (p premier), c'est en particulier un espace vectoriel de dimension n sur son sous-corps premier, isomorphe à $\mathbb{F}_p$. *A fortiori*, le groupe additif de K est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^n$.

2. Le groupe multiplicatif $\mathbb{F}_7^\times$

1. D'après le cours, $\mathbb{F}_7^\times$ est un groupe cyclique de cardinal 6. Il a donc $\varphi(6) = 2$ générateurs.
2. Un simple calcul donne les ordres suivants (pour faire effectivement les calculs à la main, il peut être bon de se rappeler que, $\mathbb{F}_7^\times$ étant isomorphe à $\mathbb{Z}/6\mathbb{Z}$, on cherche en plus de l'élément neutre 1 un élément d'ordre 2, deux d'ordre 3 et deux d'ordre 6) :

x	1 mod 7	2 mod 7	3 mod 7	-3 mod 7	-2 mod 7	-1 mod 7
ordre de x	1	3	6	3	6	2

3. Un isomorphisme $\mathbb{Z}/6\mathbb{Z} \to \mathbb{F}_7^\times$ s'obtient en envoyant k mod 6 sur a^k mod 7 pour un certain générateur a de $\mathbb{F}_7^\times$ (souvenons-nous que $\mathbb{Z}/6\mathbb{Z}$ est noté additivement mais $\mathbb{F}_7^\times$ l'est multiplicativement). En choisissant $a = 3$ mod 7, on obtient par exemple l'isomorphisme :

$x \in \mathbb{Z}/6\mathbb{Z}$	0 mod 6	1 mod 6	2 mod 6	3 mod 6	4 mod 6	5 mod 6
$\varphi(x) \in \mathbb{F}_7^\times$	1 mod 7	3 mod 7	2 mod 7	-1 mod 7	-3 mod 7	-2 mod 7

3. Automorphismes de $\mathbb{F}_4$

Le corps $\mathbb{F}_4$ peut être construit comme le quotient $\mathbb{F}_2[X]/(X^2+X+1)$. Notons $\omega \in \mathbb{F}_4$ l'image de X. Si $\varphi : \mathbb{F}_4 \to \mathbb{F}_4$ est un isomorphisme, on doit avoir

$$\varphi(\omega)^2 + \varphi(\omega) + 1 = \varphi(\omega^2 + \omega + 1) = \varphi(0) = 0.$$

Réciproquement, si $\zeta \in \mathbb{F}_4$ est une racine de X^2+X+1, le morphisme $\text{év}_\zeta : \mathbb{F}_2[X] \to \mathbb{F}_4$ passe au quotient en un morphisme

$$\overline{\text{év}_\zeta} : \mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1) \to \mathbb{F}_4,$$

qui est un morphisme de corps. Un tel morphisme est nécessairement injectif, et, comme $\mathbb{F}_4$ est fini, il est alors automatiquement bijectif.

En résume, on a une bijection

$$\begin{array}{ccc} \text{Aut}(\mathbb{F}_4) & \to & \left\{ \zeta \in \mathbb{F}_4 \,\middle|\, \zeta^2 + \zeta + 1 = 0 \right\} \\ \varphi & \mapsto & \varphi(\omega). \end{array}$$

qui envoie d'ailleurs $\mathrm{id}_{\mathbb{F}_4}$ sur ω. Remarquons que le cours nous fournit un autre automorphisme : le morphisme de Frobenius $x \mapsto x^2$ qui est associé par notre bijection à $\omega^2 = 1+\omega$.

Il nous reste donc à chercher les racines de X^2+X+1 dans $\mathbb{F}_4$. Il n'y a en fait rien à faire puisque d'après ce qui précède, ω et $1+\omega$ en sont et qu'il ne saurait y en avoir plus (la vérification directe de ce fait étant de toute façon immédiate).

Il y a donc deux isomorphismes de corps de $\mathbb{F}_4$: l'identité et le morphisme de Frobenius $x \mapsto x^2$.

Évidemment, la portée de cet argument est bien plus grande que le cas particulier de $\mathbb{F}_4$. On peut démontrer avec cette méthode que le groupe $\mathrm{Aut}(\mathbb{F}_{p^n})$ est le groupe cyclique de cardinal n engendré par l'automorphisme de Frobenius $x \mapsto x^p$.

4. Polynômes irréductibles de petits degrés sur $\mathbb{F}_2$

Un polynôme sur $\mathbb{F}_2$ ne peut avoir que deux racines : 0 et 1. Il admet la racine 0 quand son coefficient constant est nul, et la racine 1 quand il a un nombre pair de monômes non triviaux. Cette remarque permet facilement de déterminer les polynômes irréductibles de degré 2 ou 3, qui sont exactement les polynômes sans racine : X^2+X+1 en degré 2 ainsi que X^3+X^2+1 et X^3+X+1 en degré 3. Pour le degré 4, un polynôme sans racine qui n'est pas irréductible se décompose en produit de deux polynômes irréductibles de degré 2, c'est donc fatalement $(X^2+X+1)^2 = (X^4+X^2+1)$. Il y a donc trois polynômes irréductibles de degré 4 sur $\mathbb{F}_2$: $X^4+X^3+X^2+X+1$, X^4+X^3+1 et X^4+X+1.

Commençons par montrer que $\mathbb{F}_2[X]/(X^3+X^2+1)$ et $\mathbb{F}_2[X]/(X^3+X+1)$ sont isomorphes. Pour cela, soit $T : \mathbb{F}_2[X] \to \mathbb{F}_2[X]$ l'isomorphisme d'anneaux défini par $T(P) = P(X+1)$. T est égal à son propre inverse. Le noyau de la composition $\pi \circ T : \mathbb{F}_2[X] \to \mathbb{F}_2[X]/(X^3+X+1)$ (π étant la surjection canonique $\mathbb{F}_2[X] \to \mathbb{F}_2[X]/(X^3+X+1)$) est donc l'ensemble des polynômes P tels que T(P) est divisible par X^3+X+1. On a alors

$$\begin{aligned} \exists Q \in \mathbb{F}_2[X] : T(P) = (X^3+X+1)\,Q \quad &\Leftrightarrow \quad \exists Q \in \mathbb{F}_2[X] : P = T(X^3+X+1)\,T(Q) \\ &\Leftrightarrow \quad \exists \widetilde{Q} \in \mathbb{F}_2[X] : P = T(X^3+X+1)\,\widetilde{Q}, \end{aligned}$$

donc $\ker(\pi \circ T) = (T(X^3+X+1)) = ((X+1)^3+(X+1)+1) = (X^3+X^2+1)$ et le théorème d'isomorphisme fournit un isomorphisme $\mathbb{F}_2[X]/(X^3+X^2+1) \simeq \mathbb{F}_2[X]/(X^3+X+1)$.

Puisque $T(X^4+X^3+1) = (X+1)^4+(X+1)^3+1 = X^4+X^3+X^2+X+1$, la même méthode marche, *mutatis mutandis*, pour démontrer $\mathbb{F}_2[X]/(X^4+X^3+1) \simeq \mathbb{F}_2[X]/(X^4+X^3+X^2+X+1)$.

En revanche, la preuve de l'isomorphisme $\mathbb{F}_2[X]/(X^4+X^3+1) \simeq \mathbb{F}_2[X]/(X^4+X+1)$ est moins évidente. Pour l'obtenir, cherchons dans $K = \mathbb{F}_2[X]/(X^4+X+1)$ une racine ζ du polynôme X^4+X^3+1. Par essais et erreurs, on obtient une des quatre solutions possibles (ici, on note ω l'image de X dans K) : $\zeta_1 = \omega^3+1$, $\zeta_2 = \omega^3+\omega+1$, $\zeta_3 = \omega^3+\omega^2+1$ et $\zeta_4 = \omega^3+\omega^2+\omega$. Quel que soit le choix effectué, on obtient un morphisme d'évaluation $\mathrm{év}_\zeta : \mathbb{F}_2[X] \to K$ qui passe au quotient en un morphisme

$$\overline{\mathrm{év}_\zeta} : \mathbb{F}_2[X]/(X^4+X^3+1) \to \mathbb{F}_2[X]/(X^4+X+1).$$

Puisque les deux polynômes sont irréductibles et de même degré, $\overline{\mathrm{év}_\zeta}$ est un morphisme de corps entre deux corps de même cardinal : c'est donc un isomorphisme.

5. Inclusion de corps finis

On utilisera l'expression courante « $\mathbb{F}_{q'}$ se plonge dans $\mathbb{F}_q$ » (en symboles : $\mathbb{F}_{q'} \hookrightarrow \mathbb{F}_q$) pour dire que $\mathbb{F}_q$ contient un sous-corps isomorphe à $\mathbb{F}_{q'}$ (puisque tout morphisme de corps est injectif, c'est équivalent à l'existence d'un morphisme $\mathbb{F}_{q'} \to \mathbb{F}_q$).

On a déjà une condition nécessaire : si $\mathbb{F}_{q'}$ se plonge dans $\mathbb{F}_q$, appelons $\mathrm{K} \subset \mathbb{F}_q$ le sous-corps isomorphe à $\mathbb{F}_{q'}$. $\mathbb{F}_q$ est alors un K-espace vectoriel. En particulier, on a $|\mathbb{F}_q| = |\mathrm{K}|^{\dim_{\mathrm{K}} \mathbb{F}_q} = (q')^{[\mathbb{F}_q:\mathrm{K}]}$. Donc *si $\mathbb{F}_{q'}$ se plonge dans $\mathbb{F}_q$, q est une puissance de q'.*

Remarquons que si $\mathbb{F}_q$ contient un sous-corps $\mathrm{K} \simeq \mathbb{F}_{q'}$, les éléments $x \in \mathrm{K}$ vérifient $x^{q'} = x$. Puisqu'il y en a exactement q', cela implique que $\mathrm{X}^{q'} - \mathrm{X}$ est scindé sur $\mathbb{F}_q$ et que les éléments de K sont exactement les q' racines dudit polynôme. En particulier, *si $\mathbb{F}_q$ contient un sous-corps $\mathrm{K} \simeq \mathbb{F}_{q'}$, il en contient un seul.*

Réciproquement, le paragraphe précédent nous fournit la clef pour construire K : si q est une puissance $(q')^n$, le polynôme $\mathrm{X}^{q'} - \mathrm{X}$ est scindé sur $\mathbb{F}_q$. En effet, $\mathbb{F}_q^\times$ est un groupe cyclique de cardinal $q - 1 = (q')^n - 1 = (q' - 1)(1 + q' + \cdots + (q')^{n-1})$. Il possède donc un sous-groupe cyclique de cardinal $q' - 1$ dont les éléments sont déjà autant de racines de $\mathrm{X}^{q'} - \mathrm{X}$. En ajoutant 0, on obtient bien q' racines dans $\mathbb{F}_q$. Soit donc K l'ensemble des racines de $\mathrm{X}^{q'} - \mathrm{X}$. Il reste à voir que K est bien un corps : puisqu'il est de cardinal q', on aura bien obtenu un plongement $\mathbb{F}_{q'} \hookrightarrow \mathbb{F}_q$. Si on note p la caractéristique de $\mathbb{F}_q$, on a un entier e tel que $q' = p^e$. L'élévation à la puissance q' n'est alors rien d'autre que la puissance Frob^e, où $\mathrm{Frob} : x \mapsto x^p$ est le morphisme de Frobenius. On vérifie alors facilement que $\mathrm{X} = \left\{ x \in \mathbb{F}_q \;\middle|\; \mathrm{Frob}^e(x) = x \right\}$ est un sous-corps de $\mathbb{F}_q$.

En résumé, $\mathbb{F}_q$ admet un sous-corps isomorphe à $\mathbb{F}_{q'}$ si et seulement si q est une puissance de q' et dans ce cas, un tel sous-corps est unique.

7. Un exemple de réciprocité quadratique

1. On sait que le groupe multiplicatif $\mathbb{F}_{p^2}^\times$ est cyclique, de cardinal $p^2 - 1 = (p+1)(p-1)$. Puisque p est impair, les deux entiers $p \pm 1$ sont pairs et l'un des deux est même multiple de 4. Leur produit $p^2 - 1$ est donc un multiple de 8 et le groupe cyclique admet un sous-groupe cyclique d'ordre 8 et $\varphi(8) = 4$ éléments α d'ordre 8. Pour chacun de ces choix, α^4 est un élément d'ordre 2 de $\mathbb{F}_{p^2}^\times$, c'est-à-dire -1. On a donc trouvé dans $\mathbb{F}_{p^2}$ quatre racines différentes de $\mathrm{X}^4 + 1$, ce qui démontre que le polynôme est scindé.
2. Si $\alpha^4 = -1$, on a $(-\alpha)^4 = \alpha^4 = -1$ et $(\pm\alpha^{-1})^4 = \alpha^{-4} = (\alpha^4)^{-1} = (-1)^{-1} = -1$: les quatre nombres sont racines de $\mathrm{X}^4 + 1$. Ils sont fatalement différents : en caractéristique impaire, seul 0 est égal à son opposé et $\alpha = \pm\alpha^{-1} \Rightarrow \alpha^2 = \pm 1 \Rightarrow \alpha^4 = 1 \neq -1$.
3. On a $(\alpha + \alpha^{-1})^2 = \alpha^2 + \alpha^{-2} + 2\alpha\alpha^{-1} = \alpha^2 + \alpha^{-2} + 2$. Or, α^2 et α^{-2} sont deux éléments d'ordre 4 de $\mathbb{F}_{p^2}^\times$ qui sont différents (s'ils étaient égaux, α^4 vaudrait 1 alors qu'il vaut -1) : or, si β est d'ordre 4, l'autre élément d'ordre 4 est $-\beta$. Nos deux nombres sont donc opposés, ce qui démontre $(\alpha + \alpha^{-1})^2 = 2$.
4. Un élément $x \in \mathbb{F}_{p^2}$ est dans le sous-corps premier $\mathbb{F}_p$ si et seulement si $x^p = x$. Puisque α est d'ordre 8 dans $\mathbb{F}_{p^2}^\times$, α^k ne dépend que du résidu de k modulo 8. On a même $\alpha^7 = \alpha^{-1}$,

$\alpha^5 = \alpha^4\alpha = -\alpha$ et donc $\alpha^3 = -\alpha^{-1}$. On a alors :

$$(\alpha+\alpha^{-1})^p = \alpha^p + \alpha^{-p} = \begin{cases} \alpha+\alpha^{-1} & \text{si } p \equiv \pm 1 \bmod 8 \\ -\alpha-\alpha^{-1} & \text{si } p \equiv \pm 3 \bmod 8 \end{cases}$$

et $\alpha+\alpha^{-1} \in \mathbb{F}_p$ si et seulement si $p \equiv \pm 1 \bmod 8$.

5. On a trouvé deux racines de X^2-2 dans $\mathbb{F}_{p^2}$, à savoir $\pm(\alpha+\alpha^{-1})$. Il n'y en a donc pas d'autre. En particulier, on peut trouver une racine carrée de 2 dans $\mathbb{F}_p$ si et seulement si ces éléments sont dans $\mathbb{F}_p$. Évidemment, soit aucun des deux n'est dans $\mathbb{F}_p$ soit ils le sont tous les deux. Bref, *2 est un carré dans* $\mathbb{F}_p$ (i.e. *modulo p*) *si et seulement si* $p \equiv \pm 1 \bmod 8$.