Université Claude Bernard Lyon 1

MASTER M1G-Algèbre

Factorisation de $X^q - X$ sur $\mathbb{F}_p$

On veut résoudre l'exercice suivant :

Exercice .0.1. Factoriser $X^{32} - X$ sur $\mathbb{F}_2$ en irréductibles.

Trève de suspense, on a

$$X^{32}-X = X(X-1)(X^5+X^3+1)(X^5+X^2+1)(X^5+X^4+X^3+X^2+1)(X^5+X^4+X^3+X+1)(X^5+X^4+X^2+X+1)(X^5+X^3+X^2+X+1)$$

"Pretty darn long, isn't it ?" Tex Avery.

La factorisation a quelque chose de fascinant : de droite à gauche, elle est quasi-triviale, il suffit de développer et de bourriner, de gauche à droite, elle est très mystèrieuse. Notez que si vous pensiez l'inverse, vous êtes soit, génial, soit, dyslexique, soit les deux.

C'est d'ailleurs exactement ce dont on a besoin dans la cryptographie : des transformations faciles à faire (le développement) et difficile à défaire (la factorisation).

Allons-y donc pour la factorisation.

***Question* 1.** Si P, irréductible divise le polynôme $X^{32} - X$ dans $\mathbb{F}_2[X]$, alors P est de degré 1 ou de degré 5.

Effectivement, soit $\mathbb{K} = \mathbb{F}_2[\alpha]$ le corps de rupture de P (on peut le faire car P est irréductible sur $\mathbb{F}_2$) et si k est le degré de P, alors $[\mathbb{K} : \mathbb{F}_2] = k$ et donc $\mathbb{K} \simeq \mathbb{F}_2^k$, ce qui implique que le cardinal de $\mathbb{K}$ est 2^k et donc par unicité des corps finis, $\mathbb{K} \simeq \mathbb{F}_{2^k}$. Or, α, qui est par construction racine de P est donc aussi racine de $X^{32} - X$, ainsi $\alpha \in \mathbb{F}_{32}$. Ceci implique que

$$\mathbb{F}_2 \subset \mathbb{K} = \mathbb{F}_{2^k} = \mathbb{F}_2[\alpha] \subset \mathbb{F}_{2^5}$$

Le corps $\mathbb{F}_{2^5}$ est de dimension d sur $\mathbb{F}_{2^k}$, on a donc $2^5 = (2^k)^d$ et donc k divise 5. Il vient que $k = 1$ ou 5.

Et réciproquement, c'est vrai ?

***Question* 2.** Si P est un polynôme irréductible de degré 1 ou 5, sur $\mathbb{F}_2$, montrer qu'il divise $X^{32} - X$.

Si P est de degré 1, on a $P = X$ ou $X - 1$, qui divise clairement $X^{32} - X$. On suppose P de degré 5. Soit α une racine de P et $\mathbb{K} = \mathbb{F}_2[\alpha]$ le corps de rupture de P sur $\mathbb{F}_2$. Alors, comme précédemment, $\mathbb{K} = \mathbb{F}_{2^5}$ et comme $\alpha \in \mathbb{K} = \mathbb{F}_{32}$, il vient que α est racine de $X^{32} - X$. Comme P est irréductible sur $\mathbb{F}_2$ annulant α, c'est le polynôme minimal de α sur $\mathbb{F}_2$, et il divise donc $X^{32} - X$.

Le polynôme $X^{32} - X$ n'a que des racines simples, puisque sa dérivée ne s'annule jamais : c'est -1 ; il n'y a donc pas de multiplicité dans la décomposition de $X^{32} - X$ en polynômes irréductibles sur $\mathbb{F}_2$. Il y a dans sa décomposition X, et $(X - 1)$, seuls polynômes de degré 1. Il reste donc $6 = \frac{32-2}{5}$ polynômes de degré 5. Quels sont ces 6 polynômes ?

***Question* 3.** Montrer que les polynômes irréductibles de degré 5 sur $\mathbb{F}_2$ sont (X^5+X^3+1), (X^5+X^2+1), $(X^5+X^4+X^3+X^2+1)$, $(X^5+X^4+X^3+X+1)$, $(X^5+X^4+X^2+X+1)$, $(X^5+X^3+X^2+X+1)$.

Pour qu'un polynôme de degré 5 soit irréductible sur $\mathbb{F}_2$, il faut et il suffit que ces deux conditions soient réalisées : 1) qu'il n'ait pas 0 ou 1 comme racine (en fait, qu'il n'ait pas de diviseur de degré 1, 2) qu'il ne se décompose pas en un polynôme irréductible de degré 2 sur $\mathbb{F}_2$ et un polynôme irréductible de degré 3 sur $\mathbb{F}_2$. Effectivement, la première condition fait qu'il n'y aura pas de polynôme de degré 1 et donc pas de polynôme de degré 4 non plus dans sa décomposition, et la seconde, fera, qu'il n'y aura pas de polynôme de degré 2 ou 3.

La première condition est équivalente au fait que le facteur de degré 0 est 1, et ensuite que le nombre de coefficients non nuls du polynôme est impair, puisque $P(1)$ vaut 0 ou 1 selon la parité du nombre de coefficients non nuls.

La seconde condition n'est pas si dure à exprimer. Le seul polynôme irréductible de degré 2 est X^2+X+1, et qu'il n'existe que deux polynômes irréductible de degré 3 sur $\mathbb{F}_2$: X^3+X+1 et X^3+X^2+1, ce qui, au passage est exprimé par les formules :

$$X^4-X=X(X-1)(X^2+X+1),\ X^8-X=X(X-1)(X^3+X+1)(X^3+X^2+1).$$

Il faut donc éliminer les polynômes réductibles suivants $(X^2+X+1)(X^3+X+1)=X^5+X^4+1$ et $(X^2+X+1)(X^3+X^2+1)=X^5+X+1$. Il ne reste donc plus que les 6 polynômes cités plus haut.

Résolution de l'exercice.

Les polynômes X, $(X-1)$, (X^5+X^3+1), (X^5+X^2+1), $(X^5+X^4+X^3+X^2+1)$, $(X^5+X^4+X^3+X+1)$, $(X^5+X^4+X^2+X+1)$, $(X^5+X^3+X^2+X+1)$ sont irréductibles, distincts, donc deux à deux premiers entre eux. Ils divisent tous $X^{32}-X$ et donc, leur produit (=leur ppcm) divise $X^{32}-X$. On a égalité par égalité des degrés.

Maintenant, on peut essayer de « partitionner »les racines de $X^{32}-X$ en racines des polynômes irréductibles de la décomposition. Il y a $\{0\}$, puis, $\{1\}$. Et ensuite le casse-tête commence. On va appeler α une racine de (X^5+X^2+1).

Soit α une racine de X^5+X^2+1. Peut-on factoriser X^5+X^2+1 totalement sur $\mathbb{F}_{32}$?

Exercice .0.2. Montrer que les racines de X^5+X^2+1 sont α, α^2, α^4, α^8, α^{16}. C'est-à-dire :

$$X^5+X^2+1=(X-\alpha)(X-\alpha^2)(X-\alpha^4)(X-\alpha^8)(X-\alpha^{16})$$

En gros, comment, à partir d'une racine, trouver toutes les autres. Voici qui va nous mettre sur la piste : Soit σ un automorphisme d'un corps $\mathbb{K}$, pour tout $P=\sum_i a_iX^i\in\mathbb{K}[X]$, on pose $P^\sigma=\sum_i\sigma(a_i)X^i\in\mathbb{K}[X]$.

***Question* 4.** Montrer que si $\beta\in\mathbb{K}$ est racine de P, alors $\sigma(\beta)$ est racine de P^σ.

$P^\sigma((\sigma(\beta))=\sum_i\sigma(a_i)\sigma(\beta)^i=\sigma(P(\beta))=\sigma(0)=0$. D'où l'assertion.

***Question* 5.** Montrer que α^2 est encore une racine de X^5+X^2+1.

On pose $\mathbb{K} = \mathbb{F}_{32}$, σ le Frobenius $x \mapsto x^2$, $\alpha = \beta$ et enfin $P = X^5 + X^2 + 1$. Comme $P \in \mathbb{F}_2[X]$, ses coefficients sont tous stables par le Frobenius. Donc, $P^\sigma = P$ et donc d'après ce qui précède, $\sigma(\alpha) = \alpha^2$ est racine de P.

Quelles sont les racines de P ?

***Question* 6.** Montrer que le Frobenius de $\mathbb{F}_{32}$ est d'ordre 5 et déduire que α, α^2, α^4, α^8, α^{16} sont tous distincts.

On note que le Frobenius, $x \mapsto x^2$, que l'on va noter desormais F, est d'ordre 5 sur $\mathbb{F}_{32}$. Effectivement, d'une part pour tout x dans $\mathbb{F}_{32}$, on a $F^5(x) = x^{2^5} = x$. Donc l'ordre de F divise 5. Or $F \neq \mathrm{Id}$ car $x^2 = x$ implique $x = 0$ ou 1. Il est bien d'ordre 5.

On a donc une action du groupe $\mathbb{Z}/5\mathbb{Z} \simeq \langle F \rangle$ sur l'ensemble des racines du polynôme $X^5 + X^2 + 1$.

Quel est le stabilisateur de α ? C'est un sous-groupe d'ordre 1 ou 5 de $\langle F \rangle$. S'il était d'ordre 5, alors on aurait α stable par F, et donc, $\alpha = 0$ ou 1, absurde. Il est d'ordre 1. Et donc l'orbite de α est de cardinal 5. Ils sont bien tous distincts.

Résolution de l'exercice. C'est fini. On a cinq racines distinctes de $X^5 + X^2 + 1$, de degré 5, donc, ce sont les seules.

En fait, et il s'agit là d'une introduction à la théorie de Galois, la partition cherchée n'est rien autre qu'une décomposition en orbites pour une action de groupe. Voilà le lien entre recherche de racines et théorie des groupes qui a révolutionné l'algèbre.

Une dernière thématique :

***Question* 7.** On vient de voir que $P := X^5 + X^2 + 1$ était irréductible sur $\mathbb{F}_2$. Est-il irréductible sur $\mathbb{F}_4$?

Soit α une racine de $P = X^5 + X^2 + 1$. Si on montre que $\mathbb{F}_4[\alpha]$ est de degré 5 sur $\mathbb{F}_4$, c'est gagné. En effet, dans ce cas, l'évaluation en α envoie $\mathbb{F}_4[X]$ surjectivement $\mathbb{F}_4[\alpha]$ et son noyau est un idéal engendré par un polynôme de degré 5, comme P est dans l'idéal, P est générateur de l'idéal. Conclusion, $\mathbb{F}_4[X]/(P)$ est le corps $\mathbb{F}_4[\alpha] = \mathbb{F}_4(\alpha)$. Donc, P est irréductible sur $\mathbb{F}_4$.

Montrons donc que $\mathbb{F}_4[\alpha]$ est de degré 5 sur $\mathbb{F}_4$, notons donc d ce degré. Notons que $d \leq 5$, puisque d est le degré du polynôme minimal de α sur $\mathbb{F}_4$, qui est forcément plus petit que 5 (le degré de P. On a les deux tours de corps

$$\mathbb{F}_2 \subset \mathbb{F}_4 \subset \mathbb{F}_4(\alpha),\ \mathbb{F}_2 \subset \mathbb{F}_2(\alpha) = \mathbb{F}_{32} \subset \mathbb{F}_4(\alpha).$$

La première tour donne $[\mathbb{F}_4(\alpha) : \mathbb{F}_2] = 2d$, par le théorème de la base téléscopique, et la seconde que 5 divise $[\mathbb{F}_4(\alpha) : \mathbb{F}_2]$. Comme 5 divise $2d$, et que 5 et 2 sont premiers entre eux, 5 divise d. Donc $d = 5$, puisque $d \leq 5$.

Plus généralement, si P est irréductible de degré m sur un corps $\mathbb{K}$, et que $\mathbb{L}$ est une extension de $\mathbb{K}$ de degré n premier avec m, alors P reste irréductible sur $\mathbb{L}$.

Pour terminer, faisons le point sur les outils utilisés.

Sur les extensions générales de corps :

1. Le théorème de la base téléscopique : dans une tour de corps $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$, on a $[\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}] = [\mathbb{M} : \mathbb{K}]$. Cela fournit un lien étroit entre théorie des corps et arithmétique.

2. Si P est irréductible de degré n sur $\mathbb{K}$, alors $\mathbb{K}[X]/(P)$ est un corps et c'est une extension de $\mathbb{K}$ de degré n.
3. Si $\mathbb{K}$ est un corps et $\mathbb{L} = \mathbb{K}(\alpha)$ une extension de degré n, alors l'évaluation en α de $\mathbb{K}[X]$ dans $\mathbb{L}$ a pour noyau un idéal principal engendré par un polynôme P de degré n, irréductible sur $\mathbb{K}$.
4. En particulier, si $Q \in \mathbb{K}[X]$ annule α, alors P divise Q.
5. Si $\mathbb{K}$ est un corps et $\mathbb{L} = \mathbb{K}(\alpha)$ une extension de degré n, et si $P \in \mathbb{K}[X]$ annule α et est de degré n, il est irréductible sur $\mathbb{K}$.

Sur les corps finis.

1. Soit $q = p^n$, avec p premier. Le corps fini $\mathbb{F}_q$ est l'ensemble des racines de $X^q - X$ dans une clôture algébrique de $\mathbb{F}_p$. En particulier, tout élément non nul de $\mathbb{F}_q$ est une racine de l'unité.
2. Structure de corps : $\mathbb{F}_q$ est de degré n sur $\mathbb{F}_p$. Additivement, $\mathbb{F}_q \simeq \mathbb{F}_p^n$ (en fait comme espace vectoriel, donc comme groupe). $(\mathbb{F}_q^*, \cdot)$ est isomorphe à $(\mathbb{Z}/(q-1)\mathbb{Z}, +)$.
3. Le Frobenius : $F : x \mapsto x^p$ est un automorphisme du corps $\mathbb{F}_q$ dont les invariants sont exactement le sous-corps $\mathbb{F}_p$. C'est un automorphisme d'ordre n.
4. Si P est un polynôme de $\mathbb{F}_p[X]$ et α une racine de P dans $\mathbb{F}_q$, alors $F(\alpha)$ est encore une racine de P.

Mieux, le groupe $\langle F \rangle$ engendré par le Frobenius agit sur l'ensemble des racines de P. Les orbites de cette action correspondent à la décomposition en irréductibles de P sur $\mathbb{F}_p$. Par exemple, si O est une orbite, alors $\prod_{\beta \in O}(X - \beta)$ est bien dans $\mathbb{F}_p[X]$ et c'est un facteur irréductible de P.