Université Rennes 1, Année 2012-2013
Master 1 Math., Algèbre générale de base

Exercices sur les extensions de corps, chapitre 3
indications de correction

Exercice 3.1

1) On doit montrer que $g = Y^4 + Y^3 + Y^2 + Y + 1$ est irréductible. Notons en préalable que le seul polynôme irréductible de $\mathbb{F}_2[Y]$ est $Y^2 + Y + 1$ (remarque : sur $\mathbb{F}_2$, tout les polynômes non nuls sont unitaires !). En effet, un polynôme de degré 2 irréductible a un coefficient constant non nul, donc égal à 1, donc il est de la forme $Y^2 + aY + 1$. Pour $a = 0$ on trouve $Y^2 + 1 = (Y + 1)^2$ non irréductible. Pour $a = 1$ on a le polynôme $Y^2 + Y + 1$ qui est sans racine, de degré ≤ 3 donc irréductible.

Supposons que $g = ij$ avec i, j polynômes non constants. Les degrés de i et j sont soit $(1, 3)$ soit $(2, 2)$. On vérifie immédiatement que g n'a pas de racine dans $\mathbb{F}_2$, donc nécessairement on est dans le cas $(2, 2)$ avec i, j irréductibles. La seule possibilité est $i = j = Y^2 + Y + 1$, or $g \neq (Y^2 + Y + 1)^2$. Donc g est irréductible et $\mathbb{F}_2[Y]/(g)$ est un corps. Ce corps K est de cardinal $2^4 = 16$.

2) Notons $\alpha = \overline{Y}$.On a $\alpha^5 - 1 = (\alpha - 1)(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1) = 0$ donc $\alpha^5 = 1$. Ainsi α est d'ordre 5 dans K^*, et comme K^* est d'ordre 15, ce n'est pas un générateur.

3) Pour trouver un générateur de K^*, soyons astucieux. Il suffirait de trouver une racine troisième de α ; celle-ci serait d'ordre 15, comme souhaité. Trouver une racine troisième de α ne semble pas immédiat. En revanche, comme $\alpha^5 = 1$ on a $\alpha^{-1} = \alpha^4 = -(\alpha^3 + \alpha^2 + \alpha + 1) = \alpha^3 + \alpha^2 + \alpha + 1$ (dans $\mathbb{F}_2$ on a $-1 = +1$). Ceci est utile car :

- l'ordre de α^{-1} est le même que celui de α, c'est-à-dire 5, et une racine troisième de α^{-1} sera donc un générateur de K^* ;
- puisque le corps de coefficients est $\mathbb{F}_2$, on a $(\alpha + 1)^3 = \alpha^3 + 3\alpha^2 + 3\alpha + 1 = \alpha^3 + \alpha^2 + \alpha + 1$.

On a fini : $\alpha + 1$ est une racine troisième de α^{-1}, donc son ordre est 15, donc il engendre K^*.

4) Pour trouver un zéro de $f = X^4 + X + 1$ dans K, on « part à la pêche ». Les éléments de K s'écrivent comme des polynômes en α de degré $d \leq 3$; on va chercher un zéro pour f comme polynôme de degré petit. On voit d'abord que f n'a pas de racine dans $\mathbb{F}_2$, donc $d = 0$ ne convient pas. Si on cherche un zéro de la forme $r + s\alpha$ avec $r, s \in \mathbb{F}_2$, on n'en trouve pas donc $d = 1$ ne donne pas non plus de zéro. Si on cherche un zéro de la forme $r + s\alpha + t\alpha^2$, on est mené à l'équation

$$r^4 + s^4\alpha^4 + t^4\alpha^8 + r + s\alpha + t\alpha^2 + 1 = 0.$$

Utilisant $\alpha^8 = \alpha^3$, $r^4 = r$, $s^4 = s$, $t^4 = t$ (noter que n'importe quel $x \in \mathbb{F}_2$ a toutes ses puissances x^n, $n \geq 1$, égales à lui-même !), on trouve une solution pour $r = s = t = 1$. Ainsi $z = 1 + \alpha + \alpha^2$ est un zéro de f. Notons maintenant $F : K \to K, x \mapsto x^2$ l'automorphisme de Frobenius de K. Alors $F(z) = z^2$, $F^2(z) = z^4$ et $F^3(z) = z^8$ sont aussi des zéros pour f. Après calcul on trouve les quatre zéros de f dans K :

$$\{1 + \alpha + \alpha^2, 1 + \alpha^2 + \alpha^4, 1 + \alpha^3 + \alpha^4, 1 + \alpha + \alpha^3\}.$$

Il en découle que le morphisme d'anneaux $\mathbb{F}_2[X] \to K$ qui envoie X sur $1+\alpha+\alpha^2$ passe au quotient en un morphisme $u : \mathbb{F}_2[X]/(f) \to K$. Or f ne possède pas de zéro dans $\mathbb{F}_2$ et est distinct de $(X^2+X+1)^2$, donc il est irréductible par le même raisonnement que celui utilisé pour g. Donc $\mathbb{F}_2[X]/(f)$ est un corps. Finalement u est un morphisme entre deux corps (donc injectif) extensions de $\mathbb{F}_2$ de degré 4 (donc surjectif) : c'est un isomorphisme.

Exercice 3.2

1) Ici K est d'ordre 9, donc K^* est d'ordre 8. On calcule $\alpha^2 = 1 + \alpha$, $\alpha^4 = 2$ et $\alpha^8 = 1$ (en fait le calcul de α^8 n'est pas nécessaire, on sait que $x^8 = 1$ pour tout $x \in K^*$ puisqu'on est dans un groupe d'ordre 8).

2) Les deux éléments $r \in \mathbb{F}_3^*$ on pour polynôme minimal $T - r$, et les éléments de K^* qui ne sont pas dans $\mathbb{F}_3^*$ sont de la forme $r + s\alpha$ avec $r, s \in \mathbb{F}_3$ et $s \neq 0$. Or il est clair que le polynôme minimal de $r + s\alpha$ est $f(s^{-1}(T - r))$. (Le point important est que $r + s\alpha$ est l'image de α par la transformation $T \mapsto r + sT$ qui est un automorphisme de l'anneau de polynômes $\mathbb{F}_3[T]$, et le polynôme minimal de $r + s\alpha$ est alors le « transformé » de celui de α par l'automorphisme inverse, qui est $T \mapsto s^{-1}(T - r)$.)

3) Le groupe K^* est isomorphe à $\mathbb{Z}/8\mathbb{Z}$, dont les générateurs sont les classes d'entiers premiers à 8, c'est-à-dire $1, 3, 5, 7$. En repassant dans K^*, ceci dit que les générateurs de K^* sont α, α^3, α^5 et α^7. On peut, si on veut, les calculer sur la base $\{1, \alpha\}$ et on trouve :

$$\{\alpha, 2\alpha + 1, 2\alpha, \alpha + 2\}$$

4) Le début est facile :

$$X^9 - X = X(X^8 - 1) = X(X^4 - 1)(X^4 + 1) = X(X - 1)(X + 1)(X^2 + 1)(X^4 + 1).$$

On voit ensuite que $X^2 + 1$ est sans racine, donc irréductible. Enfin, en cherchant si $X^4 + 1$ est irréductible, on voit que c'est le produit de $X^2 + X + 2$ par $X^2 + 2X + 2$. Finalement

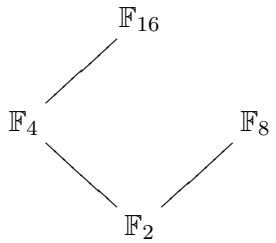
$$X^9 - X = X(X - 1)(X + 1)(X^2 + 1)(X^2 + X + 2)(X^2 + 2X + 2).$$

C'est le produit de tous les polynômes irréductibles de $\mathbb{F}_3[X]$ de degré diviseur de 2. Ce n'est pas un hasard !

Exercice 3.6

1) Remarque préliminaire : lorsqu'on agrandit le corps de coefficients, la décomposition en facteurs irréductibles devient de plus en plus fine, c'est-à-dire qu'elle possède de plus en plus de facteurs, avec des multiplicités de plus en plus grandes. En effet, si $P \in K[X]$ et $K \subset L$ est une extension de corps, alors les facteurs irréductibles de la décomposition de P dans $K[X]$ ne restent a priori pas irréductibles dans $L[X]$; chacun d'entre eux se décompose dans $L[X]$ en facteurs irréductibles, et on obtient ainsi une décomposition pour P dans $L[X]$ plus fine que dans $K[X]$.

2) Dans l'exercice présent, les inclusions de corps impliquées sont :



et il n'y a pas d'autres inclusions entre ces corps, puisque $\mathbb{F}_{q'}$ est une extension de $\mathbb{F}_q$ si et seulement si q' est une puissance de q. Pour résoudre l'exercice, le plus simple est de commencer par factoriser $X^{16} - X$ dans $\mathbb{F}_2[X]$ puis de regarder comment la factorisation obtenue se comporte (i.e. se raffine) par extension à $\mathbb{F}_4$ et $\mathbb{F}_8$. On sait d'après le cours (corollaire 3.17) que $X^{16} - X$ est le produit de tous les polynômes irréductibles unitaires de $\mathbb{F}_2[X]$ dont le degré divise 4, i.e. de degrés $1, 2$ et 4. Rappelons

simplement qu'en degré 4 les polynômes irréductibles unitaires sont ceux qui n'ont pas de racine et qui sont distincts de $(X^2+X+1)^2$. On trouve :

$$X^{16}-X = X(X-1)(X^2+X+1)(X^4+X+1)(X^4+X^3+1)(X^4+X^3+X^2+X+1).$$

3) Passons à la factorisation dans $\mathbb{F}_4[X]$. On notera F l'automorphisme de Frobenius des corps en jeu, i.e. l'élévation au carré. On a besoin d'une manière de représenter $\mathbb{F}_4[X]$; par exemple écrivons $\mathbb{F}_4[X] = \mathbb{F}_2(\beta)$ avec β racine de X^2+X+1, donc $\mathbb{F}_4 = \{0, 1, \beta, \beta+1\}$. Notons que β et $\beta+1$ sont images par F l'un de l'autre ; dans la suite ce sera d'ailleurs plus léger de noter β^2 au lieu de $\beta+1$. On a maintenant besoin de connaître les polynômes irréductibles unitaires de degré $\leq 1, 2$ de $\mathbb{F}_4[X]$, pour savoir si les trois polynômes de degré 4 qui apparaissent ci-dessus restent irréductibles dans $\mathbb{F}_4[X]$. En degré 1 c'est clair. En degré 2 il s'agit de polynômes de la forme X^2+rX+s sans racine avec r, s dans $\mathbb{F}_4$. Après un petit calcul on trouve que la condition d'être sans racine se traduit par la condition que s est distinct de $0, 1+r, 1+\beta(1+r), r+\beta(1+r)$. On trouve alors les six polynômes correspondant à

$$(r,s) \in \Big\{(1,\beta)\ ,\ (1,\beta^2)\ ,\ (\beta,1)\ ,\ (\beta,\beta)\ ,\ (\beta^2,1)\ ,\ (\beta^2,\beta^2)\Big\}.$$

Maintenant notons que les trois polynômes irréductibles de $\mathbb{F}_2[X]$ de degré 4 que l'on a ci-dessus sont sans racine dans $\mathbb{F}_4$. En effet, soit P l'un d'entre eux, on sait que P est sans racine dans $\mathbb{F}_2$; par ailleurs si β (ou β^2) est racine de P, alors son image par Frobenius l'est aussi, donc le produit $(X+\beta)(X+\beta^2)$, qui n'est rien d'autre que X^2+X+1, divise P dans $\mathbb{F}_4[X]$, auquel cas il divise P dans $\mathbb{F}_2[X]$ (rappelons que le quotient et le reste pour une DE dans $\mathbb{F}_4[X]$ de deux polynômes de $\mathbb{F}_2[X]$ sont dans $\mathbb{F}_2[X]$), ce qui n'est pas le cas.

Donc si P se scinde dans $\mathbb{F}_4[X]$, c'est en produit de polynômes irréductibles de degré 2. Pour aller plus loin, on rappelle la remarque suivante : si $\mathbb{F}_2 \subset L$ est une extension finie et si un élément $\alpha \in L$ est racine d'un polynôme $P \in \mathbb{F}_2[X]$, alors $F(\alpha)$ est aussi racine. On utilisera la variante suivante de la remarque : si $Q \in L[X]$ divise $P \in \mathbb{F}_2[X]$ dans $L[X]$, alors $F(Q)$ divise aussi P dans $L[X]$, où $F(Q)$ désigne le polynôme obtenu à partir de Q en prenant le Frobenius de tous ses coefficients. La preuve de cette remarque est élémentaire : comme F est un automorphisme de corps, alors $P = QR$ implique $F(P) = F(Q)F(R)$, or $F(P) = P$.

On exploite la remarque en disant que si $P = X^2+X+\beta$ divise l'un des trois polynômes irréductibles de $\mathbb{F}_2[X]$ de degré 4, alors $F(P) = X^2+X+\beta^2$ le divise aussi. Partons des six polynômes de $\mathbb{F}_4[X]$ de degré 2 trouvés ci-dessus et multiplions-les par leur image par Frobenius. On trouve :

$$\begin{aligned}
&(X^2+X+\beta)(X^2+X+\beta^2) = X^4+X+1,\\
&(X^2+\beta X+1)(X^2+\beta^2 X+1) = X^4+X^3+X^2+X+1,\\
&(X^2+\beta X+\beta)(X^2+\beta^2 X+\beta^2) = X^4+X^3+1.
\end{aligned}$$

On voit que chacun des trois polynômes de degré 4 se scinde dans $\mathbb{F}_4[X]$ en produit de facteurs de degré 2, et la factorisation de $X^{16}-X$ dans $\mathbb{F}_4[X]$ est :

$$\begin{aligned}
X^{16}-X = X(X-1)(X+\beta)(X+\beta^2)(X^2+X+\beta)(X^2+X+\beta^2)\\
\times (X^2+\beta X+1)(X^2+\beta^2 X+1)(X^2+\beta X+\beta)(X^2+\beta^2 X+\beta^2).
\end{aligned}$$

4) Montrons enfin que la factorisation dans $\mathbb{F}_8[X]$ est simplement :

$$X^{16}-X = X(X-1)(X^2+X+1)(X^4+X+1)(X^4+X^3+1)(X^4+X^3+X^2+X+1),$$

c'est-à-dire que chacun des facteurs de la factorisation dans $\mathbb{F}_2[X]$ reste irréductible sur $\mathbb{F}_8$. D'abord X^2+X+1 n'a pas de racine dans $\mathbb{F}_8$, car si $\alpha \in \mathbb{F}_8$ était racine, le morphisme $\mathbb{F}_2[X] \to \mathbb{F}_8$ qui envoie

X sur α induirait un morphisme de corps $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2+X+1) \to \mathbb{F}_8$ or il n'existe pas de tel morphisme. Donc X^2+X+1 est irréductible sur $\mathbb{F}_8$. Maintenant soit P l'un des trois polynômes ci-dessus, de degré 4 et irréductibles sur $\mathbb{F}_2$. Alors P n'a pas de racine dans $\mathbb{F}_8$ car une telle racine α donnerait naissance à un morphisme $\mathbb{F}_{16} \simeq \mathbb{F}_2[X]/(P) \to \mathbb{F}_8$ qui envoie la classe de X sur α, or il n'existe pas de tel morphisme. La seule possibilité pour que P ne soit pas irréductible sur $\mathbb{F}_8$ est qu'il se scinde en produit de deux polynômes de degré 2. Ceci ne peut pas se passer, car si $Q \in \mathbb{F}_8[X]$ est un polynôme irréductible de degré 2 qui divise P, alors l'une quelconque de ses racines γ (dans une clôture algébrique) engendre un corps extension de degré 2 de $\mathbb{F}_8$, donc isomorphe à $\mathbb{F}_{64}$. Or γ est racine de P qui est de degré 4, donc $\mathbb{F}_2(\gamma)$ est de degré 4 sur $\mathbb{F}_2$, isomorphe à $\mathbb{F}_{16}$, et on a une contradiction.

Exercice 3.7

Choisissons une représentation $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$ avec α racine de $P = X^3+X+1$. Les autres racines de P dans $\mathbb{F}_8$ sont α^2 et α^4, et on note que $\alpha^4 = \alpha^2+\alpha$. Dans $\mathbb{F}_8[X]$ on a donc :

$$P = (X+\alpha)(X+\alpha^2)(X+\alpha+\alpha^2).$$

Soit x un élément de $\mathbb{F}_8$, que l'on peut écrire $x = r+s\alpha+t\alpha^2$ sur la base $\{1,\alpha,\alpha^2\}$.

Si $x \in \mathbb{F}_2$ i.e. $s=t=0$, alors son polynôme minimal est $X-r$.

Si $x \in \mathbb{F}_2$, c'est-à-dire si $st \neq 0$, alors son polynôme minimal est de degré distinct de 1. Comme le degré divise 3, alors c'est 3. Or, on a :

$$P(X+r) = (X+r+\alpha)(X+r+\alpha^2)(X+r+\alpha+\alpha^2).$$

On en conclut que le polynôme minimal de α, α^2 et $\alpha+\alpha^2$ est $P(X)$, et le polynôme minimal de $1+\alpha$, $1+\alpha^2$ et $1+\alpha+\alpha^2$ est $P(X+1)$.

Exercice 3.10

Le cardinal de K est 125 et le polynôme minimal de β est $f(X-1)$.

Exercice 3.11

1) Les deux polynômes X^2+X+2 et X^2+2 sont sans racine dans $\mathbb{F}_5$.

2) Soit $P = X^2+X+2$. On vérifie que $P(\beta^6) \neq 0$ donc il n'existe pas de morphisme de corps $f_1 : k_1 \to k_2$ tel que $f_1(\alpha) = \beta^6$.

On vérifie que $P(2\beta+2) = 0$ donc il existe un (unique !) morphisme de corps $f_2 : k_1 \to k_2$ tel que $f_2(\alpha) = 2\beta+2$. C'est un morphisme entre deux corps, donc il est injectif, et ces corps sont de même cardinal, donc f_2 est bijectif. C'est un isomorphisme.