linéaires, donc possède des racines dans K'. Ainsi, comme on l'a vu précédemment (9.1.2), K se plonge dans K'. □

La notation $\mathbf{F}_q$ et ses dangers

Soit q une puissance d'un nombre premier. Comme on vient de le voir, il n'y a essentiellement qu'un corps fini à q éléments. On s'autorise parfois de cela pour noter $\mathbf{F}_q$ un corps indéterminé à q éléments. Cette notation est dangereuse pour la raison que nous allons expliquer. Dans le cas d'un nombre premier p, si K et K' sont deux corps à p éléments, il n'y a aucun danger à écrire $K = K' = \mathbf{F}_p$, car il n'y a qu'une façon de faire se correspondre les éléments de K et les éléments de K' : à 1_K correspond $1_{K'}$, à 2_K correspond $2_{K'}$, ... Cela n'est pas vrai lorsque le nombre des éléments n'est plus premier.

Prenons comme exemple celui des corps à 4 éléments. Soit K un tel corps. Il contient le sous-corps premier $\mathbf{F}_2$, dont les éléments sont 0 et 1, et deux autres éléments, disons α et β. On a $\alpha + \alpha = 2\alpha = 0$ et de même $\beta + \beta = 0$. Puisque $\alpha + 1$ ne peut être ni 0, ni 1, ni α, on a forcément $\alpha + 1 = \beta$, donc $\beta + 1 = \alpha$. De même, on a forcément $\alpha^2 = \beta$, $\beta^2 = \alpha$ et $\alpha\beta = 1$, et on a déterminé totalement les tables d'addition et de multiplication.

EXERCICE 9.20. [A] — Les trois anneaux $\mathbf{Z}/4\mathbf{Z}$, $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$ et K sont deux à deux non isomorphes.

EXERCICE 9.21. [C] — Y a-t-il d'autres anneaux à quatre éléments que les trois ci-dessus (bien entendu, on raisonne à isomorphisme près) ?

Cela étant, il n'y a aucun moyen de distinguer l'un de l'autre les éléments α et β. Si K' est un autre corps à 4 éléments, et si on note γ et δ ses deux éléments distincts de 0 et 1, il y a deux façons distinctes d'identifier K et K'. On peut décider d'égaler K à K' de façon que $\alpha = \gamma$ et $\beta = \delta$, ou que $\alpha = \delta$ et $\beta = \gamma$.

REMARQUE 9.27. — On notera d'ailleurs que ce problème se pose déjà dans le cas du corps $\mathbf{C}$, où l'on ne peut algébriquement distinguer i de $-i$.

Cette situation se reproduit dans tous les cas : si l'on a deux corps K et K' de même nombre d'éléments $q = p^n$ et si l'on a identifié K à K' par l'application $f : K \to K'$, on peut aussi bien le faire par l'application $x \mapsto f(x)^p = f(x^p)$ par exemple. C'est l'existence de l'*automorphisme* non identique $x \mapsto x^p$ de K qui est la cause de nos ennuis.

Il s'agit là d'un phénomène très général en mathématiques. On peut souvent définir un objet par des propriétés caractéristiques, ce qui signifie que deux objets possédant ces propriétés sont isomorphes. Mais il faut prendre garde lorsque cet isomorphisme n'est pas uniquement déterminé. C'est ainsi que l'on parle d'objets « uniques à isomorphisme près » ou « uniques à isomorphisme unique près ». Par exemple, le corps à 3 éléments est unique à isomorphisme unique près, mais « le » corps à 4 éléments ne l'est pas.

En résumé, il faut être très prudent lorsqu'on abrège l'expression « K est un corps à q éléments » par $K = \mathbf{F}_q$. Sinon par exemple, ayant écrit $K = \mathbf{F}_q$, puis $K' = \mathbf{F}_q$, on en tire $K = K'$, ce qui, étant donnés des éléments x de K et x' de K', amène à la question interdite : a-t-on $x = x'$?

Tout ceci n'est pas du purisme, et traduit une difficulté pratique considérable : si on veut calculer effectivement dans un corps fini, disons $\mathbf{F}_{256}$, il faut bien être capable d'en nommer les éléments et de les manipuler. La méthode la plus naturelle (que l'on pourrait appeler « additive »), c'est de choisir un polynôme irréductible P de degré 8 sur $\mathbf{F}_2$ (on sait qu'il en existe, mais il faut en trouver un — et aussi savoir comment on discute avec celui qui en a choisi un autre !) et de prendre pour $\mathbf{F}_{256}$ le quotient $\mathbf{F}_2[X]/(P)$ correspondant. Une autre solution (« multiplicative » celle-là) est d'identifier $\mathbf{F}_{256}^*$ au groupe cyclique $\mathbf{Z}/255\mathbf{Z}$, ce qui revient à choisir une racine primitive 255-ième dans le corps inconnu[5], puis à déterminer la table d'addition. On peut combiner ces deux approches, en choisissant comme polynôme P un polynôme *primitif*, facteur irréductible de Φ_{255} dans $\mathbf{F}_2[X]$. Nous expliquerons dans le paragraphe suivant cette méthode sur l'exemple un peu plus maniable de $\mathbf{F}_{16}$.

9.3.4. Racines de l'unité dans un corps fini

Soit k un corps fini, à q éléments et soit n un entier premier à q. Un corps K contenant k est appelé une *extension cyclotomique de niveau n de k* s'il possède n racines n-ièmes de l'unité, ce qui signifie aussi qu'il possède une racine primitive n-ième de l'unité, et s'il est minimal pour cette propriété. Cela signifie donc qu'il est obtenu par adjonction à k d'une racine primitive n-ième de l'unité. Le polynôme minimal d'une telle racine primitive est un facteur irréductible dans $k[X]$ du polynôme cyclotomique Φ_n. Or on a déterminé précédemment (proposition 9.17) le degré r d'un tel facteur, et il en résulte que le corps K a q^r éléments. Il est donc bien déterminé à isomorphisme près, ce qui permet de le noter $R_n(k)$, avec le même danger que celui qu'on a signalé pour $\mathbf{F}_{p^r} = R_{p^r-1}(\mathbf{F}_p)$. En résumé :

PROPOSITION 9.28. — *Soit k un corps fini à q éléments, et soit n un entier positif premier à q. Alors le corps* $R_n(k)$ *a* q^r *éléments, où r est l'ordre de l'élément q dans le groupe* $(\mathbf{Z}/n\mathbf{Z})^*$.

Prenons par exemple $q = 2$. Alors q est d'ordre 4 à la fois modulo 5 et modulo 15. On a donc $R_5(\mathbf{F}_2) = \mathbf{F}_{16}$ et aussi $R_{15}(\mathbf{F}_2) = \mathbf{F}_{16}$.

EXERCICE 9.22. [A] — Que dit la proposition pour $n = 2$?

Prenons $n = 3$; on a $\Phi_3 = X^2 + X + 1$. D'après ce qui précède, il revient au même de dire que $X^2 + X + 1$ est irréductible dans $k[X]$, ou que $R_3(k)$ a

5. Il y en a en fait $\varphi(255) = \varphi(3)\varphi(5)\varphi(17) = 2 \times 4 \times 16 = 128$.