Exercices

1. Combien d'anneaux (commutatifs) d'ordre 4 est-qu'il y a ? (Indication : Considérer les eventuels homomorphismes surjectifs $\mathbb{Z} \to R$ ou $\mathbb{F}_2[x] \to R$.)

2. Montre que r divise $\varphi(p^r - 1)$. Plus généralement, pour tout entier $a > 1$ et $r \geq 1$, démontrer que r divise $\varphi(a^r - 1)$. (Indication : utiliser le théorème de Lagrange.)

3. Trouver les premiers p et les entiers $r \geq 1$ tel qu'il existe un seul polynôme primitif de degré r dans $\mathbb{F}_p[x]$.

4. Montrer qu'il existe un polynôme irréductible de degré r dans $\mathbb{F}_p[x]$ pour tout premier p et entier r.

5. Montrer qu'il existe un polynôme primitif de degré r dans $\mathbb{F}_p[x]$ pour tout premier p et entier r.

6. Démontrer l'unicité du corps de q éléments en le décrivant comme corps de décomposition de $x^q - x$.

7. Montrer que $x^p - x - a$ est irréductible dans $\mathbb{F}_p[x]$ pour tout a dans $\mathbb{F}_p^*$.

8. Déterminer la factorisation de $\Phi_7(x)$ dans $\mathbb{F}_2[x]$.

9. Décrire les éléments primitifs de $\mathbb{F}_{2^3}/\mathbb{F}_2$ et de $\mathbb{F}_{2^3}^*$ en termes de racines des polynômes cyclotomiques.

10. Déterminer la factorisation de $\Phi_{15}(x)$ dans $\mathbb{F}_2[x]$.

11. Décrire les éléments primitifs de $\mathbb{F}_{2^4}/\mathbb{F}_2$ et de $\mathbb{F}_{2^4}^*$ en termes des racines des polynômes cyclotomiques.

12. Trouver des isomorphismes :

$$\mathbb{F}_2[\zeta_{15}] = \mathbb{F}_2[x]/(x^4 + x + 1) \longrightarrow \mathbb{F}_2[\zeta_5] = \mathbb{F}_2[x]/(x^4 + x^3 + x^2 + x + 1),$$

et

$$\mathbb{F}_2[\zeta_{15}] = \mathbb{F}_2[x]/(x^4 + x + 1) \longrightarrow \mathbb{F}_2[\zeta_{15}] = \mathbb{F}_2[x]/(x^4 + x^3 + 1).$$

13. Montrer que $\phi(\alpha) = \alpha^p$ est un homomophisme d'anneaux $A \to A$ pour tout anneau A de caractéristique p premier. Il s'appelle l'endomorphisme de Frobenius (ou l'automorphisme de Frobenius lorsqu'il est un isomorphisme).

14. Montrer que tout homorphisme d'un corps K est injectif, et conclure que l'endomorphisme de Frobenius est un automorphisme dans le cas d'un corps fini.

15. Soit $\phi : \mathbb{F}_q \to \mathbb{F}_q$ l'automorphisme de Frobenius, où $q = p^r$. Déterminer les éléments fixés par ϕ et par ϕ^r.

16. Démontrer que $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \langle\phi\rangle$, un groupe cyclique d'ordre r.