Université de Bretagne Occidentale
UFR Sciences et Techniques
LICENCE DE MATHEMATIQUES

ARITHMETIQUE ET APPLICATIONS, COMBINATOIRE ET GRAPHES

Contrôle continu, le 7 avril 2014, 9h00–9h30

CORRIGE ET BAREME

Question de cours. (2 pts) Soit K un corps fini. Soit K_0 son sous-corps premier. On sait que $K_0 = \mathbb{Q}$ ou $K_0 = \mathbb{F}_p$ avec p premier. Comme K_0 est fini également, $K \neq \mathbb{Q}$ et donc $K = \mathbb{F}_p$. La restriction de la loi de multiplication $K \times K \to K$ au sous-ensemble $\mathbb{F}_p \times K$ fait de K un $\mathbb{F}_p$-espace vectoriel. Comme K est fini, c'est un $\mathbb{F}_p$-espace vectoriel de dimension finie. Soit n sa dimension. Comme $0 \neq 1$ dans K, l'espace vectoriel K n'est pas de dimension 0, i.e., $n \in \mathbb{N}^\star$. D'àprès le cours d'algèbre linéaire, il existe un isomorphisme linéaire entre K et $\mathbb{F}_p^n$. En particulier, K est en bijection avec $\mathbb{F}_p^n$. On en déduit que

$$|K| = |\mathbb{F}_p^n| = |\mathbb{F}_p|^n = p^n.$$

Exercice 1. a. **(1 pt)** On évalue P en $-1, 0, 1$ dans $\mathbb{F}_3$ et on obtient

$$P(-1) = P(1) = 2 \neq 0 \quad \text{et} \quad P(0) = 1 \neq 0.$$

Du coup, P n'a pas de racine dans $\mathbb{F}_3$. Comme $\deg(P) \leq 3$, cela suffit pour en déduire l'irréductibilité de P dans $\mathbb{F}_3[X]$.

b. **(1 pt)** On calcule

$$P(\alpha) = \alpha^2 + 1 = (\bar{X})^2 + 1 = \overline{X^2 + 1} = 0$$

dans $K = \mathbb{F}_3[X]/(P)$, où $\overline{(\cdot)}$ signifie la classe modulo P. Il s'ensuit que P possède une racine dans K. Comme $\deg(P) \geq 2$, cela suffit pour conclure que P est réductible dans $K[X]$.

c. **(1 pt)** En faisant la division longue de P par $X - \alpha$ on obtient la décomposition de P en facteurs irréductibles

$$P = (X - \alpha)(X + \alpha)$$

dans $K[X]$.

d. **(1 pt)** Montrons d'abord que la famille $1, \alpha$ est libre. Supposons que $\lambda \cdot 1 + \mu \cdot \alpha = 0$ avec $\lambda, \mu \in \mathbb{F}_3$. Cela veut dire que

$$0 = \lambda + \mu\bar{X} = \overline{\lambda + \mu X}$$

dans $K = \mathbb{F}_3[X]/(P)$. Du coup, le polynôme P divise $\lambda + \mu X$ dans $\mathbb{F}_3[X]$. Comme le premier est de degré 2 et le dernier est de degré 1, ce dernier est nul, i.e., $\lambda = \mu = 0$. Cela montre que la famille $1, \alpha$ est libre.

Montrons ensuite que la famille $1, \alpha$ est génératrice du $\mathbb{F}_3$-espace vectoriel K. Soit $v \in K = \mathbb{F}_3[X]/(P)$. On a donc $v = \bar{V}$ avec $V \in \mathbb{F}_3[X]$. d'après la division euclidienne, on peut écrire $V = QP + R$ avec $Q, R \in \mathbb{F}_3[X]$ et $\deg(R) < 2$. Ecrire $R = \lambda + \mu X$ avec $\lambda, \mu \in \mathbb{F}_3$. On a alors

$$v = \bar{V} = \overline{QP + R} = \overline{R} = \overline{\lambda + \mu X} = \lambda + \mu \bar{X} = \lambda \cdot 1 + \mu \cdot \alpha.$$

Cela montre que la famille $1, \alpha$ est génératrice.

Par conséquent, la famille $1, \alpha$ est une base du $\mathbb{F}_3$-espace vectoriel K.

e. **(1 pt)** D'après le d, K est en bijection avec $\mathbb{F}_3^3$ et possède donc 9 éléments. Son groupe multiplicatif $K^\times$ est donc de cardinal 8.

f. **(1 pt)** D'après le cours, $K^\times$ est cyclique. Il est donc isomorphe à $\mathbb{Z}/8\mathbb{Z}$ d'après le e. Or, le nombre de générateurs de $\mathbb{Z}/8\mathbb{Z}$ est de

$$\varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 4.$$

g. **(1 pt)** On a $\alpha^2 = -1$ et donc $\alpha^4 = 1$. L'élément α n'est donc pas générateur de $K^\times$.

h. **(1 pt)** Comme on a aussi $(-\alpha)^4 = 1$, les 4 éléments $1, -1, \alpha, -\alpha$ de $K^\times$ ne sont pas générateurs de $K^\times$. L'ensemble des générateurs de $K^\times$ est donc contenu dans le complémentaire de $\{1, -1, \alpha, -\alpha\}$ dans $K^\times$. Ce complémentaire compte 4 éléments. Comme l'ensemble des générateurs de $K^\times$ en compte 4 également, tout élément de $K^\times$ différent de $\pm 1, \pm\alpha$ en est générateur, par exemple $\alpha + 1$.