Université de Bretagne Occidentale
UFR Sciences et Techniques
L3 DE MATHEMATIQUES

ARITHMÉTIQUE ET APPLICATIONS

Contrôle continu, le 22 mars 2022, 8h00-8h30

CORRIGÉ et BARÊME

Exercice 1. a. Comme $\mathbb{F}_5^\star$ est cyclique d'ordre 4, il possède $\varphi(4) = 2$ générateurs. Comme $(\pm\bar{1})^2 = \bar{1}$, les deux éléments $\pm\bar{1}$ ne sont pas générateurs. Du coup, les deux éléments restants $\pm\bar{2}$ sont tous les deux générateurs de $\mathbb{F}_5^\star$. **(3 pts)**

b. Comme $\deg(P) = 2$, il suffit de vérifier que P ne possède pas de racine dans $\mathbb{F}_5$. Or,

$$\begin{aligned}\bar{0}^2 - \bar{2} &= -\bar{2} \neq \bar{0}\\ (\pm\bar{1})^2 - \bar{2} &= \bar{1} - \bar{2} = -\bar{1} \neq \bar{0}\\ (\pm\bar{2})^2 - \bar{2} &= \bar{4} - \bar{2} = \bar{2} \neq \bar{0}\end{aligned}$$

dans $\mathbb{F}_5$. Par conséquent, P ne possède pas de racine dans $\mathbb{F}_5$. **(3 pts)**

c. Comme P est irréductible dans $\mathbb{F}_5[X]$, l'anneau quotient $\mathbb{F}_5[X]/(P)$ est un corps **(1 pt)**. C'est aussi un $\mathbb{F}_5$-espace vectoriel de dimension $\deg(P) = 2$. Il est, en tant que tel, isomorphe au $\mathbb{F}_5$-espace vectoriel standard de dimension 2 à savoir $\mathbb{F}_5^2$. En particulier, les ensembles $\mathbb{F}_5[X]/(P)$ et $\mathbb{F}_5^2$ sont en bijection. Comme le dernier possède 25 éléments, le premier en possède autant **(2 pts)**.

d. On a

$$\delta^8 = (\delta^2)^4 = \bar{2}^4 = \bar{1}$$

car $\bar{2} \in \mathbb{F}_5^\star$ est un élément d'un groupe d'ordre 4. Du coup, l'ordre de δ est un diviseur de 8 **(1 pt)**. Les diviseurs positifs de $8 = 2^3$ sont $1, 2, 4, 8$. Si δ était d'ordre strictement inférieur à 8, on aurait $\delta^4 = \bar{1}$ dans tous les cas car 1 et 2 divisent 4. Or,

$$\delta^4 = (\delta^2)^2 = \bar{2}^2 = \bar{4} \neq \bar{1}$$

dans $\mathbb{F}_{25}$. Par consquent δ est bien d'ordre 8 dans $\mathbb{F}_{25}^\star$ **(2 pts)**.

e. L'élément $\bar{1}$ de $\mathbb{F}_{25}$ est bien-sûr racine de Q **(1 pt)**. Les autres racines de Q sont donc racine du polynôme $R = X^2 + X + \bar{1}$ qui est de discriminant

$$\Delta = \bar{1}^2 - \bar{4} \times \bar{1} \times \bar{1} = -\bar{3} = \bar{2} = \delta^2.$$

Du coup, les racines de R dans $\mathbb{F}_{25}$ sont

$$(-\bar{1} + \delta) \times (\bar{2} \times \bar{1})^{-1} \text{ et } (-\bar{1} - \delta) \times (\bar{2} \times \bar{1})^{-1}.$$

Comme $\bar{2}^{-1} = \bar{3}$ dans $\mathbb{F}_5$ et donc aussi dans $\mathbb{F}_{25}$, les racines de R dans $\mathbb{F}_{25}$ sont

$$-\bar{3} + \bar{3}\delta \text{ et } -\bar{3} - \bar{3}\delta,$$

i.e.,

$$\bar{2}+\bar{3}\delta \text{ et } \bar{2}+\bar{2}\delta \quad \textbf{(2 pts)}.$$

On a trouvé 3 racines de Q dans $\mathbb{F}_{25}$ à savoir

$$\bar{1}=\bar{1}+\bar{0}\delta,\ \bar{2}+\bar{3}\delta,\ \bar{2}+\bar{2}\delta.$$

Elles sont bien distinctes car $\bar{1}, \delta$ est une base du $\mathbb{F}_5$-espace vectoriel $\mathbb{F}_5[X]/(P)$.

f. On prend $\varepsilon=\bar{2}+\bar{2}\delta$. Comme ε est racine de $Q=X^3-\bar{1}$, on a $\varepsilon^3=\bar{1}$. L'ordre de ε est donc un diviseur de 3 **(1 pt)**. Comme 3 est premier, les seuls diviseurs positifs de 3 sont 1 et 3. Or, on a observé ci-dessus que ε n'est pas égal à l'élément neutre $\bar{1}$ de $\mathbb{F}_{25}^{\star}$. Son ordre est donc différent de 1 **(1 pt)**. Par consquent, ε est d'ordre 3.

g. Il s'agit de montrer que $\alpha=\delta\varepsilon$ est d'ordre 24 dans $\mathbb{F}_{25}^{\star}$ car $\mathbb{F}_{25}^{\star}$ est un groupe d'ordre 24. On peut vérifier par un calcul que $\alpha^i\neq\bar{1}$ pour tous les diviseurs propres de 24, ou mieux, pour les diviseurs propres maximaux de 24 à savoir 8 et 12 . Il est plus aisé de montrer directement que $\alpha^i=\bar{1}$ implique que i est un multiple de 24, ce qui suffit pour conclure. Supposons donc que $\alpha^i=\bar{1}$ pour un certain $i\in\mathbb{Z}$. On a, en particulier,

$$\bar{1}=\bar{1}^8=(\alpha^i)^8=(\alpha^8)^i=(\delta^8\varepsilon^8)^i=(\bar{1}\times\varepsilon^8)^i=\varepsilon^{8i}$$

car $\delta^8=\bar{1}$. Comme ε est d'ordre 3, on en déduit que $3|8i$. Comme 3 et 8 sont premiers entre eux, on obtient $3|i$. De même

$$\bar{1}=\bar{1}^3=(\alpha^i)^3=(\alpha^3)^i=(\delta^3\varepsilon^3)^i=(\delta^3\times\bar{1})^i=\delta^{3i}$$

car $\varepsilon^3=\bar{1}$. Comme δ est d'ordre 8, on en déduit que $8|3i$, et que $8|i$. Du coup, i est multiple de 3 et de 8 et donc multiple de $\mathrm{ppcm}(3,8)=24$ [1]. **(3 pts)**

1. C'est un fait général : si x et y sont deux éléments commutants d'un groupe d'ordre m et n respectivement, avec m et n premiers entre eux, alors xy est d'ordre mn.