

ARITHMÉTIQUE ET APPLICATIONS, COMBINATOIRE ET
GRAPHES

Examen terminal, le 12 mai 2014, 14h00–17h00

Documents et calculatrices sont interdits.

Question de cours. Soit L/K une extension finie de corps. Montrer que tout élément de L est algébrique sur K .

Exercice 1. Soit $F = \sum a_n X^n$ l'unique série formelle dans $\mathbb{C}[[X]]$ telle que

$$X(D(XF)) = F - 1,$$

où $D(F)$ désigne la dérivée formelle F' de F .

- Déterminer a_n pour tout $n \in \mathbb{N}$.
- La série formelle F appartient-elle au sous-anneau $\mathbb{C}[X]$ des polynômes en X ?
- La série formelle F est-elle une fraction rationnelle en X ?
- La série formelle F est-elle inversible dans l'anneau $\mathbb{C}[[X]]$?

Exercice 2. Pour n un entier naturel, soit a_n le nombre de couples $(x, y) \in \mathbb{N}^2$ tels que $2x + 3y = n$. Soit F la série génératrice $\sum a_n X^n$ dans $\mathbb{Q}[[X]]$.

- Montrer que F est égale à la fraction rationnelle

$$\frac{1}{(1 - X^2)(1 - X^3)}.$$

- Déterminer la décomposition en éléments simples de F dans $\mathbb{C}(X)$.
- En déduire une formule close pour a_n , pour tout $n \in \mathbb{N}$.

Exercice 3. Déterminer le 15-ième polynôme cyclotomique Φ_{15} sur \mathbb{Q} .

Exercice 4. Soit $P = X^4 + X + 1$ dans $\mathbb{F}_2[X]$.

- Montrer que P est irréductible dans $\mathbb{F}_2[X]$.

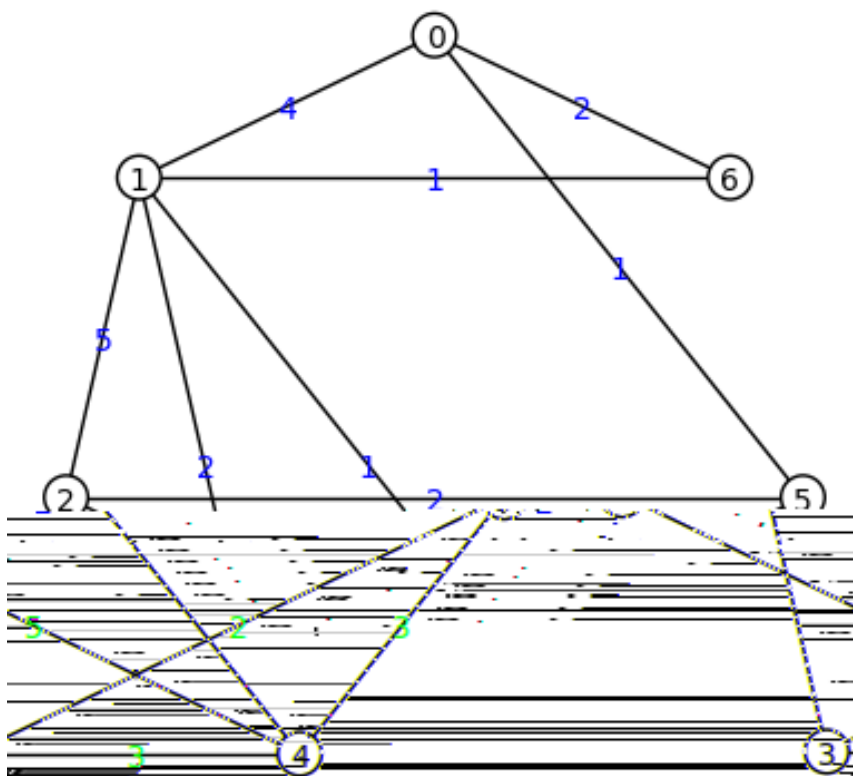
Soit K le corps $\mathbb{F}_2[X]/(P)$ et désignons par α la classe de X modulo P dans K .

- Montrer que la famille $1, \alpha, \alpha^2, \alpha^3$ est une base du \mathbb{F}_2 -espace vectoriel K .
- Quel est le cardinal du groupe multiplicatif K^* ?
- Montrer que α est un générateur de K^* .

Alice et Bob veulent convenir d'une clé secrète partagée en suivant le procédé Diffie-Hellman. Alice et Bob décident d'utiliser $G = K^*$ comme groupe et $g = \alpha$ comme générateur. Alice envoie le message $A = \alpha^3 + \alpha + 1$ à Bob, et Bob envoie le message $B = \alpha^2 + 1$ à Alice.

e. Déterminer la clé secrète d'Alice et Bob.

Exercice 5. Soit G le graphe pondéré ci-dessous. Déterminer, à l'aide de l'algorithme de Dijkstra, le chemin le plus court dans G du sommet 0 à n'importe quel autre sommet de G .



Barème indicatif sur 20 points :

Q de cours	2 pts
Exercice 1	4 pts
Exercice 2	4 pts
Exercice 3	2 pts
Exercice 4	5 pts
Exercice 5	3 pts

T. S. V. P.