UFR de Mathématiques et Informatique
Université Bordeaux I

Année 1999–2000

Licence de Mathématiques et Informatique

Module d'Algorithmique Algébrique

Devoir surveillé du 24 novembre 1999

Durée 3 heures

Documents interdits. Le barême n'est qu'indicatif.

Exercice I (8 points)

Le but de cet exercice est de déterminer à isomorphisme près tous les groupes de cardinal 10.

On rappelle le résultat vu en cours et en T.D. : si tous les éléments d'un groupe fini G vérifient $x^2 = e$ (où e est l'élément neutre du groupe) alors G est abélien et son cardinal est une puissance de 2.

Soit tout d'abord G un groupe *non cyclique* de cardinal 10.

1) En utilisant le résultat rappelé ci-dessus, montrer que si G est un groupe non cyclique de cardinal 10 il possède un élément d'ordre 5.

Dans toute la suite on notera a un élément d'ordre 5, et $H =< a >$ le groupe d'ordre 5 engendré par a. Enfin, on notera b un élément de G n'appartenant pas à H.

2) a) Rappeler pourquoi H est distingué dans G et $G = H \cup bH$ (réunion disjointe).
b) En déduire que G est engendré par a et b.

3) a) En considérant le groupe quotient G/H montrer que $b^2 \in H$.
b) En considérant b^6, montrer que b ne peut pas être d'ordre 5.
c) En déduire que b est d'ordre 2.

4) a) Expliquer pourquoi ba est aussi un élément d'ordre 2.
b) En déduire que G est un groupe engendré par deux éléments a et b d'ordre 5 et 2 respectivement et vérifiant $bab^{-1} = a^{-1}$.
c) En déduire que le groupe G est isomorphe au groupe diédral D_5 des isométries d'un pentagone régulier.

5) Donner la liste complète des groupes d'ordre 10 à isomorphisme près.

Exercice II (11 points)

On considère les sous-ensembles $\mathbb{Z}[i]$ et $\mathbb{Q}(i)$ du corps $\mathbb{C}$ des nombres complexes définis de la manière suivante :

$$\mathbb{Z}[i] = \{a + bi/\ a, b \in \mathbb{Z}\} \qquad \text{et} \qquad \mathbb{Q}(i) = \{a + bi/\ a, b \in \mathbb{Q}\}\ .$$

1) Montrer brièvement que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$ et que $\mathbb{Q}[i]$ est un sous-corps de $\mathbb{C}$ contenant $\mathbb{Z}[i]$.

2) On rappelle que l'on note $\lfloor x \rceil$ l'entier le plus proche d'un réel x et que $|x - \lfloor x \rceil| \leq 1/2$. Montrer que pour tout $z \in \mathbb{C}$, il existe $\alpha \in \mathbb{Z}[i]$ tel que $|z - \alpha| \leq \sqrt{2}/2$, où ici bien sûr $|z|$ désigne le module du nombre complexe z.

3) a) Soient α et β dans $\mathbb{Z}[i]$ avec $\beta \neq 0$. En appliquant ce qui précède à $z = \alpha/\beta$, montrer qu'il existe $q \in \mathbb{Z}[i]$ tel que $|\alpha - q\beta| < |\beta|$.

b) En déduire que $\mathbb{Z}[i]$ est un anneau euclidien, de stathme $|z|^2$. Pourquoi $|z|$ n'est-il pas un stathme tel que défini dans le cours ?

4) Donner la liste des éléments inversibles de $\mathbb{Z}[i]$. En déduire que pour tout élément $\alpha \in \mathbb{Z}[i]$ non nul, il existe un et et seul élément associé à α (c'est à dire de la forme αu avec u inversible) appartenant au premier quadrant (nombres complexes d'argument appartenant à $[0, \pi/2[$).

5) On pose $\alpha = 38 + 44i$, $\beta = 22 + 31i$. Expliciter complètement l'algorithme d'Euclide sur α et β, en effectuant les divisions euclidiennes en utilisant la méthode décrite ci-dessus (bien entendu les quotients sont dans $\mathbb{Z}[i]$ et pas nécessairement dans $\mathbb{Z}$). En déduire l'unique PGCD δ de α et β appartenant au premier quadrant.

6) (Question facultative) En utilisant l'algorithme d'Euclide étendu (version naïve ou non), calculer u et v dans $\mathbb{Z}[i]$ tels que $\alpha u + \beta v = \delta$.

Exercice III (6 points)

On appelle *nombre de Mersenne* un nombre de la forme $M_n = 2^n - 1$ avec $n \geq 2$.

1) a) Montrer que si n est pair, M_n est premier si et seulement si $n = 2$.

b) Montrer que si $n \geq 3$ est impair et que $n = ab$ avec $a > 1$ et $b > 1$, alors M_n est divisible par M_a et M_b.

c) En déduire que si M_n est premier alors nécessairement n est premier

2) Soit p un nombre premier et q un diviseur *premier* de M_p (éventuellement M_p lui-même si M_p est premier).

a) Soit G le groupe $(\mathbb{Z}/q\mathbb{Z})^*$ des éléments inversibles modulo q. Montrer que l'ordre de la classe de 2 dans G (c'est-à-dire le plus petit entier strictement positif k tel que $2^k \equiv 1 \pmod{q}$) est égal à p.

b) En utilisant le petit théorème de Fermat pour q, en déduire que p divise $q - 1$.

c) Déduire de ce qui précède que *tout* diviseur de M_p est congru à 1 modulo $2p$.

3) De la question précédente appliquée à $p = 11$, on déduit que $q = 23$ est le plus petit nombre premier qui a une chance de diviser M_{11}.

a) Calculer le plus intelligemment possible le reste de la division euclidienne de 2^{11} par 23.

b) En déduire que M_{11} n'est pas un nombre premier, donc que la réciproque de la question 1)c) est fausse.

Remarque. La recherche des nombres de Mersenne premiers est très difficile. On en connait moins de 40, le plus grand ayant plusieurs *millions* de chiffres.

Exercice IV (5 points)

Soit P un polynôme de terme dominant $a_m X^m$ et de racines α_i, et Q un polynôme de terme dominant $b_n X^n$ et de racines β_j. On rappelle que le résultant de P et Q est donné par les formules

$$R(P,Q) = a_m^n \prod_{1 \leq i \leq m} Q(\alpha_i) = (-1)^{mn} b_n^m \prod_{1 \leq j \leq n} P(\beta_j) \ .$$

Calculer explicitement le résultant de deux polynômes généraux du second degré $P(X) = a_1 X^2 + b_1 X + c_1$ et $Q(X) = a_2 X^2 + b_2 X + c_2$, où $a_1 \neq 0$ et $a_2 \neq 0$. Le résultat doit être un polynôme en les a_i, b_i et c_i et ne doit pas faire intervenir de racines carrées.