M1 MEEF PLC Maths – Rennes 1 et ESPE Bretagne
GEA2 – Compléments d'Algèbre, géométrie et algorithmique (II) 2016-2017

Contrôle des connaissances Au cours de la 4^{e}, de la 8^{e} et de la 12^{e} séance, un contrôle continu de 30 minutes sera donné. Il portera sur tout ce qui a pu être vu au cours de l'ensemble des séances précédentes. Chacun de ces contrôles fournira une note **N_i**. A l'issue de l'enseignement il y aura un contrôle continu de rattrapage. Il durera 120 minutes (tiers-temps compris, donc 90 minutes sans tiers-temps). Il fournira une note **R**. La note finale F sera calculée de la façon suivante: **F=1/n[max(N_1,R)+...+max(N_n,R)]** où n est le nombre de contrôles continus de 30 mn donnés.

Modifications d'emploi du temps Il est conseillé de lire régulièrement son courrier électronique et son environnement numérique de travail pour ne pas manquer un changement d'emploi du temps.

Agenda

30/01 (2h). Exercices 1 à 6. Les exercices 7 et 13 sont à préparer pour le 02/02. Il est à noter que la tentative de pavage esquissée au tableau pour résoudre l'exercice 6 est à corriger pour obtenir un pavage périodique qui permette d'établir le théorème de Pythagore.

02/02 (2h). Exercices 7 et 10 (bijection de N dans Z, de N dans NxN, reste à faire bijection de N dans Q et absence de bijection de N dans R). Les exercices 13 et 14 sont à préparer pour le 06/02. Il est indiqué qu'il sera demandé lors du contrôle du 09/02 de donner une démonstration du théorème de Pythagore par pavage, de traiter l'exercice 10 du recueil d'exercices et de traiter un exercice qui sera fait le 06/02.

06/02 (2h). Fin de l'exercice 10 (bijection de N dans Q et absence de bijection de N dans R). Exercices 13 et 14 (sauf l'analyse des 7 dernières lignes de l'algorithme). L'exercice 63 est à préparer pour le 09/02.

09/02 (2h). Avant de traiter l'exercice 63 l'étude d'invariants utiles à l'étude de configurations du jeu de solitaire est réalisée. Un collégien, en stage de 3 jours dans l'UFR Mathématiques réalise un introduction au sujet. L'exercice 63 est corrigé (en fait imparfaitement car l'énoncé doit être modifié pour que l'exercice soir réalisable). La séance s'achève par le contrôle continu 1.

14/02 (2h). Les copies corrigées du contrôle continu 1 sont rendues. Des précisions sont données sur l'exercice 63. La séance est surtout consacrée à une révision de quelques notions et elle est illustrée d'exemples : relation, relation réflexive, symétrique, antisymétrique, transitive, d'ordre, d'équivalence, classes d'équivalence, loi de composition interne, loi associative, commutative, neutre, inverse, unicité du neutre, inverse, unicité de l'inverse, groupe, sous-groupe, construction de Z, de Z/nZ. L'exercice 15 est à préparer pour le 16/02.

16/02 (2h). L'exercice 15 n'a pu être traité et il est donc à préparer pour le 28/02. En guise d'introduction à la docimologie il a été dit pourquoi le théorème de la limite centrale, ou même plus simplement la loi faible des grands nombres, pouvait expliquer pourquoi la moyenne d'une suite (assez longue) de notes, même incertaines, convergeait vers une note « absolue ». Il a aussi été expliqué aussi que la moyenne de 5 notes, chacune incertaine à 1 près, pouvait avec une probabilité de 40 % (respectivement de 20%) être inférieure ou égale à 9,8 (respectivement à 9,4) alors que sans incertitude la moyenne aurait au moins de 10. Chacun est invité à le vérifier expérimentalement à l'aide de son tableur favori. On montre pendant la séance que la loi qui à n et m dans N associe |a-b| est commutative, admet un neutre mais n'est pas associative. On montre aussi comment à partir d'une loi et d'une bijection on peut (artificiellement) en construire une deuxième. L'exemple de la loi 2+xy-x-y construite à partir de la multiplication et de la bijection 1+x

de R est exploré. Des exemples de groupes sont donnés (quelconque, commutatif, fini, fini commutatif, fini non commutatif). Le groupe S3 des permutations de {1,2,3} est décortiqué et différentes façons de l'observer, en particulier des façons qui s'appuient sur une vision géométrique, sont données. C'est l'occasion de rappeler par écrit ce qu'est une application linéaire et d'expliquer le distinguo entre espace vectoriel (le monde des vecteurs) et espace affine (le monde des points). C'est aussi l'occasion d'expliquer sur des exemples comment passer des permutations à des matrices. Le prochain contrôle continu aura lieu le 02/03 et il portera sur le jeu de Nim à plusieurs tas (savoir jouer les coups gagnants quand c'est possible et savoir quand c'est possible d'en jouer), sur les notions de relation, de loi et de groupe.

28/02 (2h). Un petit rappel sur le produit de matrices est fait. L'exercice 15 est traité de façon détaillée. Il s'agit de comprendre, grâce à la division euclidienne dans Z, que les idéaux de Z sont ses sous-groupes, les sous-ensembles du type nZ. Il est donné des exemples d'anneaux dont les sous-groupes ne sont pas en général des idéaux. Il est aussi expliqué pourquoi la division euclidienne dans R[X] permet de montrer que tout idéal de cet anneau a un seul générateur. Il est montré qu'a contrario ce n'est pas vrai dans Z[X]. Il est demandé de préparer les exercices 18 et 19 pour le 02/03, séance qui se terminera par un contrôle continu dont le programme a été précisé (jeu de Nim à plusieurs tas (savoir jouer les coups gagnants quand c'est possible et savoir quand c'est possible d'en jouer), notions de relation, de loi et de groupe).

02/03 (2h). En guise d'introduction on donne une preuve de l'irrationalité de la racine de 2 en montrant « géométriquement » que s'il existe deux carrés C0 et C1 à côtés entiers et tels que l'aire de C0 est le double de celle de C1 alors il existe deux carrés C3 et C5 strictement plus petits et vérifiant les mêmes propriétés. On aborde ensuite l'exercice 18. On discute, après avoir résolu l'exercice et avant d'avoir débuté le contrôle continu de l'ordre partiel sur l'ensemble des entiers naturels non nuls selon lequel un entier est inférieur ou égal à un autre s'il le divise. Il est demandé de poursuivre la préparation de l'exercice 19 qui n'a pu être traité en séance.

06/03 (2h). Des éléments de correction du contrôle continu sont donnés. L'exercice 19 est traité ainsi que l'exercice 34 (lemme de Gauss) et la question de l'exercice 42 sur le petit théorème de Fermat. Il est rappelé que le 3^{e} contrôle continu aura lieu jeudi 16 mars.

09/03 (2h). Avant de traiter les exercices 42 puis 41 sur le petit théorème de Fermat une preuve géométrique de l'irrationalité de la racine carrée de 2 reposant sur des constructions de triangles est donnée ainsi que deux preuves algébriques du même résultat. La première de ces preuves algébriques est l'exercice 37 qui permet d'établir un résultat général sur les entiers qui admettent des racines entières. C'est l'occasion de montrer que si p premier avec q divise q^n alors p=1. La seconde est une preuve plus élémentaire qui repose sur le fait que les puissances d'un nombre impair sont toujours impaires. Chaque fois on mesure la puissance du lemme de Gauss. Des petites remarques sur la commutativité et l'associativité sont données et il est fait observer rapidement que la série de terme général (-1)^n/n, bien que convergente, n'est pas commutativement convergente, ni absolument convergente. Il est précisé que le prochain contrôle continu, prévu jeudi 16 mars portera sur l'irrationalité de la racine de 2, sur Bezout, Gauss, la division euclidienne, les pgcd et Fermat. Il est conseillé de préparer l'exercice 43 pour la séance du 13 mars (attention c'est lundi à 8h) et pour le contrôle du 16 mars.

13/03 (2h). Les exercices 43 (petit théorème de Fermat en utilisant l'indicatrice d'Euler), 22 (algorithme d'Euclide pour trouver l'identité de Bezout) et 27 (théorèmes des restes chinois, questions1, 2, 3, 4 et 10). Des exemples numériques sont donnés. Il est demandé de regarder pour le 16/03 les exercices 31, 32, 33, 50 et 65. Il est rappelé que le 3^{e} contrôle continu aura lieu jeudi 16 mars.

16/03 (2h). Les exercice 31, 32 et 33 sont traités (infinité des ensembles des nombres premiers et des nombres premiers congrus à 3 modulo 4, algorithme pour trouver les nombres premiers inférieurs ou égaux à un entier naturel premier). Il est expliqué pourquoi tout entier est le produit d'un nombre fini de nombres premiers mais l'unicité de la décomposition n'est pas établie (il aurait fallu résoudre l'exercice 38), il est juste indiqué qu'elle est une conséquence du lemme de Gauss. Les exercices 50 et 65 qui n'ont pu être abordés en séance sont à regarder pour le 21/03. Il est précisé que le sujet du contrôle continu terminal (de 90 minutes, le 30 mars probablement) sera organisé de la façon suivante :
- exercice 1 (4 pts) (injection de Q dans Z, loi commutative non associative, idéal non principal de Z[X], algorithme pour rechercher les nombres premiers inférieurs ou égaux à un entier donné) ;
- exercice 2 (1 pt) (pour un entier, posséder une racine carré rationnelle implique d'être un carré) ;
- exercice 3 (3 pts) (petit théorème de Fermat par le binôme de Newton) ;
- exercice 4 (7 pts) (infinité des ensembles des nombres premiers, des nombres premiers congrus à 3 modulo 4 et des nombres premiers congrus à 1 modulo 4) ;
- exercice 5 (3 pts) (construction d'une suite décroissante vers 0 de réels strictement positifs et appartenant à un sous-groupe de R dès que ce sous-groupe contient 1 et un nombre irrationnel) ;
- exercice 6 (2 pts) (algorithme permettant d'obtenir l'identité de Bezout et application sur un exemple).

21/03 (2h). Il est montré que si p1,…,pk sont des nombres premiers différents alors 1/p1+...+1/pk n'est pas un entier (question 4 de l'exercice 23). Il est aussi montré que 1+1/2+...+1/n n'est pas un entier (question 8 de l'exercice 40). La notion de valuation 2-adique est abordée. Les questions 6, 7 et 8 de l'exercice 27 sont traitées. C'est l'occasion d'expliquer la correspondance entre générateurs de Z/nZ et nombres premiers à l'entier n. On termine la séance en montrant comment paramétrer l'ensemble des points à coordonnées rationnelles du cercle unité (exercice 50).

23/03 (2h). La fin de l'exercice 50 est traitée. Il s'agit de résoudre dans Z^3 l'équation a^2+b^2=c^2. Il est montré qu'on obtient toutes les solutions (a,b,c) (dans N^3) avec pgcd(a,b,c)=1 en considérant les triplets (2pq, p^2-q^2, p^2+q^2) et (p^2-q^2, 2pq, p^2+q²) avec p>q des entiers naturels premiers entre eux et de parités différentes. L'exercice 65 sur le chiffrement RSA de Rivest, Shamir et Adleman est traité. C'est l'occasion d'évoquer rapidement la question du calcul de a^m dans Z/nZ en faisant un nombre réduit de multiplications (l'exponentiation rapide qui est l'objet de l'exercice 62). Ceci constitue la dernière séance d'enseignement. La prochaine séance, programmée le 30 mars, sera celle du contrôle continu terminal (de 90 minutes).