Université d'Évry Val d'Essonne 2011-2012

M54 algèbre et arithmétique 2

Plan du cours

(version du 10 décembre 2011)

Les cours et TD ont lieu le lundi de 9h45 à 13h en salle 118 à l'IBGBI ; ils commencent et terminent la même semaine. Voici la correspondance entre numéro de semaine et jours du calendrier :

1. 19 sept.	4. 10 oct.	7. 18 nov. [1]	10. 2 déc. [1]	13. 2 janv.
2. 26 sept.	5. 7 nov.	8. 21 nov.	11. 5 déc.	
3. 3 oct.	6. 14 nov.	9. 28 nov.	12. 12 déc.	

Le contrôle continu est constitué d'un DS et d'un DM. Le DS a eu lieu en semaine 6 ; un DM a été distribué en semaine 9, à rendre en semaine 12. La note de contrôle continu sera le maximum entre la note de DS et la moyenne (arithmétique, non pondérée) des notes de DS et DM.

L'examen est prévu le 16 janvier de 10h à 13h. La note finale du module sera le maximum entre le note d'examen et la moyenne (arithmétique, non pondérée) des notes d'examen et de contrôle continu.

(sem. 1) **Introduction**

Rappels sur les lois de composition internes et leurs propriétés. Définitions des structures algébriques usuelles : monoïdes, groupes, anneaux, corps, modules, espaces vectoriels. Exemples. Lien entre lois et « opérations ».

I Anneaux, corps : notions fondamentales

I.1 Définitions et exemples de base. Opérations sur les anneaux : fonctions à valeurs dans un anneau, matrices à coefficients dans un anneaux, polynômes, anneaux produits.

Groupe des inversibles. Éléments simplifiables, diviseurs de zéro ; exemples dans $\mathbf{Z}/n\mathbf{Z}$ et les anneaux produits. Anneaux intègres.

Puissances entières dans les anneaux et entières relatives dans les corps. Remarque : pas de racines en général. Éléments nilpotents, idempotents. Exemples dans $M_n(\mathbf{Z})$, $\mathbf{Z}/n\mathbf{Z}$ et les anneaux produits.

(sem. 2) **I.2 Morphismes.**

1. En rattrapage des séances manquées (17 et 31 oct.), de 14h à 17h15, salle habituelle.

Définition, critère pratique, exemples, contre-exemple : application nulle. La composée de deux morphismes en est un. La réciproque d'un morphisme bijectif en est un. Rappel : endo, iso, auto.

I.3 Sous-anneaux, sous-corps. Définitions, critères pratiques ; exemples, contre-exemple : l'anneau nul. Intersection de sous-anneaux, l'union et la somme de sous-anneaux ne sont pas des sous-anneaux. Anneau engendré par une partie.

Rappel : images directes et réciproques d'ensembles par des applications. Les images directes et réciproques de sous-anneaux par des morphismes sont des sous-anneaux. Définitions : image et noyau d'un morphisme ; l'image est un sous-anneau, par le noyau.

(sem. 3) **I.4 Idéaux.**

Motivation : noyau ; définition et première propriété : les noyaux sont des idéaux. Exemples : idéaux triviaux, $n\mathbf{Z}$ et idéaux principaux, anneaux de fonctions. Différences avec les sous-anneaux. Un corps a exactement deux idéaux.

Opérations : intersection, idéal engendré par une partie finie (expression explicite, généralise les idéaux principaux), somme, produit. Idéal des nilpotents. Image réciproque par un morphisme, mais pas directe ($\mathbf{Z} \hookrightarrow \mathbf{Q}$).

(sem. 4) **I.5 Quotients.**

Théorème-définition : anneau quotient et surjection canonique. Exemples : quotients triviaux, $\mathbf{Z}/n\mathbf{Z}$. Passage d'un morphisme au quotient. Exemple : $\mathbf{Z}/mn\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$. Théorème d'isomorphisme. Exemple : $\mathbf{C}$ comme quotient de $\mathbf{R}[X]$.

II Arithmétique dans Z et ses quotients

(sem. 5) Rappel : relation de Bézout et PGCD. Inversibles de $\mathbf{Z}/n\mathbf{Z}$, calcul d'inverses, équations $ax = b \mod n$. Théorème chinois classique et étendu, systèmes de congruences.

(sem. 6) *DS portant sur le programme des 5 premières semaines.*

(sem. 7) Retour sur $(\mathbf{Z}/n\mathbf{Z})^\times$: fonction ϕ d'Euler, théorème d'Euler et petit théorème de Fermat.

Notions de cryptosystèmes symétriques (ex : César) et asymétriques (analogie : adresse email et mot de passe), avantages et inconvénients : gestion des clés, taille des clés. Le cryptosystème RSA.

(sem. 8) Notion d'anneau euclidien ; $\mathbf{Z}$ est euclidien. Notion d'anneau principal (c-ex : $k[X, Y]$) ; les anneaux euclidiens sont principaux. Interprétation en termes d'idéaux du PGCD et du PPCM dans un anneau principal. (Interprétation de la divisibilité en termes d'idéaux, produits d'idéaux principaux.)

Idéaux premiers et maximaux : définitions naïves. Idéaux premiers et maximaux de $\mathbf{Z}$. Caractérisation des idéaux premiers et maximaux en termes de quotient ; les idéaux maximaux sont premiers.

(sem. 9) Notion d'éléments associés et égalité des idéaux engendrés. Notion d'éléments irréductibles. Lemme de Gauss dans un anneau principal. Notion d'anneau factoriel. $\mathbf{Z}[i\sqrt{3}]$

n'est pas factoriel. Les anneaux principaux sont factoriels (lemme : la réunion d'une suite croissante d'idéaux est un idéal). Pour la culture : $k[X, Y]$ est factoriel mais pas principal.

DM : démonstration du théorème des deux carrés en utilisant les propriétés de $\mathbf{Z}[i]$.

III Anneaux de polynômes en une variable, extensions de corps, corps finis

(sem. 10) Rappel degré et division euclidienne ; $\mathbf{Z}[X]$ n'est pas euclidien. PGCD, PPCM, Bézout, décomposition en facteurs irréductibles dans $K[X]$; polynômes unitaires et normalisation. Racines d'un polynôme : multiplicité, nombre de racines distinctes. Irréductibilité et racines dans $K[X]$. Lemme de Gauss.

(sem. 11) Rappel : notion d'algèbre ; un morphisme donne un structure d'algèbre ; $K[X]$ et ses quotients sont des algèbres. $K[X]/(P)$ est de dimension (finie) $\deg P$; c'est un corps ssi P est premier ; calcul d'inverses.

Caractéristique d'un anneau, d'un corps ; morphisme de Frobenius ; le cardinal d'un corps fini est une puissance d'un nombre premier. Tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique (admis) ; le groupe multiplicatif d'un corps fini est cyclique. Tout corps fini est un quotient de $\mathbf{F}_p[X]$. Existence et unicité du corps à p^n éléments (admis). Condition d'existence d'un morphisme $\mathbf{F}_q \to \mathbf{F}_{q'}$ (suffisance admise).

(sem. 12) Problème du logarithme discret et applications à la cryptographie : Diffie-Hellman, ElGamal.

(sem. 13) *Correction du DM et révisions : sujet de septembre 2011 et retour sur les exercices non traités en TD les semaines précédentes.*