Programme du partiel d'algèbre générale.

Le partiel porte sur l'ensemble du cours.

1) Arithmétique élémentaire (développement des entiers et des rationnels en base b inclus)

2) Dénombrements: pour une révision vous pouvez consulter ma fiche de rappel (disponible sur ce site) sur les principes de dénombrements, les exemples et formules types (nombre d'applications, formules binomiale et multinomiale,...) et quelques exercices corrigés.

[Les nombres de Catalan (récurrence et fonction génératrice) du cours ne sont pas au prgm du partiel]

3) Dénombrabilité: se limiter à ce qui a été fait en cours. Pour une révision vous pouvez consulter ma fiche - Cardinalité - disponible sur ce site.

[A l'exception du lemme de Cantor, qui implique que les ensembles

$$P(N), P(P(N)), P(P(P(N))), \dots$$

sont non équipotents et non dénombrables, les sections 'Ensembles non dénombrables' et 'Cardinaux' de cette fiche ne sont pas au programme du partiel.]

4) Groupes:
Certains points d'arithmétique et groupes sont repris dans ma fiche - Questions d'arithmétique - disponible sur ce site.
Le corrigé du problème 2 de l'écrit zéro 2011 est une lecture utile et conseillée sur ces questions.

Puisqu'il s'agit d'un chapitre important voici une liste des notions et résultats principaux:

- sous groupes de $(Z,+)$, preuve de Bézout sous la forme $a_1Z+a_2Z+\ldots+a_nZ = \text{pgcd}\,(a_1,\ldots,a_n)Z$.

- Sous-groupe $\langle P\rangle$ engendré par une partie P d'un groupe G. [Pour des exemples matriciels voir le corrigé du partiel de janvier 2011, exercice 2, question 3 et le corrigé du partiel de novembre 2012 exercice 4. Si nécessaire, réviser la multiplication et l'inversion des matrices!]

- Ordre d'un élément. Groupes monogènes (par ex. $(Z,+)$) et cycliques (par ex. $(Z/nZ,+)$, le groupe $(U_n,\times)$ des racines $n-$ièmes de l'unité dans le plan complexe).

- Le nombre de générateurs d'un groupe cyclique d'ordre n = l'indicatrice d'Euler $\varphi(n)$.

- Le groupe des inversibles multiplicatifs $A^\star$ d'un anneau A en particulier $((Z/nZ)^\star,\times)$. [Dans le problème 2 de l'ecrit zéro 2011 distribué en cours, $A^\star$ est noté $U(A)$.]

- Groupe produit. Le produit $G\times G'$ est cyclique ssi G et G' sont cycliques d'ordres étrangers.

- Table d'un groupe fini.

- Classes à gauche pour un sous-groupe $H<G$. Passage au quotient d'une application.
Théorème de Lagrange: l'ordre de tout sous-groupe H d'un groupe fini G est un diviseur de l'ordre de G, en particulier l'ordre de tout élément de G est un diviseur de l'ordre de G.
Application du thm de Lagrange au groupe $(Z/nZ)^\star$: soit $a\in Z\setminus\{0\}$ et $\varphi(n)$ l'indicatrice d'Euler. Si pgcd $(a,n)=1$ alors $a^{\varphi(n)}\equiv 1[n]$. Cas particulier: si un nombre premier p ne divise pas a alors $a^{p-1}\equiv 1[p]$ (petit théorème de Fermat).

- Morphismes de groupes. Sous-groupe distingué. Noyau et image d'un morphisme.

- Tout groupe cyclique d'ordre n est isomorphe à Z/nZ.

- Isomorphisme entre groupes finis par comparaison des tables.

- Tout isomorphisme de groupes conserve l'ordre des éléments.

- Tout sous groupe d'un groupe cyclique est cyclique. Pour tout diviseur d de l'ordre (i.e. du cardinal) d'un groupe cyclique G il existe un unique sous-groupe d'ordre d dans G.

- Le théorème des restes chinois (version groupe/anneau): Si $a_1, \ldots, a_n$ sont des entiers naturels non nuls 2 à 2 premiers, alors

$$Z/a_1a_2\cdots a_nZ \simeq Z/a_1Z \times \cdots \times Z/a_nZ \quad \text{(isomorphisme d'anneaux)}$$

- Les groupes étudiés en détail: $(Z/nZ, +)$ et/ou $(U_n, \times)$ et le groupe non commutatif S_n des permutations de $[1, n]$.

Pour un autre exemple utile, voir l'étude détaillée des groupes $((Z/2^kZ)^\star, \times)$ dans le corrigé de l'écrit zéro 2011 Problème 2.

- Groupes et géométrie: l'exemple fait en cours des groupes d'isométries de R^3 conservant chaque axe de coordonnées ou la réunion de ces axes figure dans ma fiche Groupes III disponible sur ce site.

- Groupe quotient par un sous-groupe distingué et théorème d'isomorphisme: $G/ker(f) \simeq Im(f)$.

5) Actions d'un groupe sur un ensemble: se limiter à la présentation du cours, savoir traiter un exemple guidé. Voici les notions vues en cours:

- Définition d'une action $\phi : G \times E \to E : (g, x) \mapsto g \cdot x$. Une action du groupe G sur l'ensemble E équivaut à un morphisme $G \to S(E)$ où $S(E)$ est le groupe des bijections de E muni de la loi de composition des applications.

- Orbites de l'action de G: pour $x \in E, Orb(x) = \{g \cdot x, g \in G\}$. Partition de E en $G-$ orbites. En particulier pour un ensemble fini E ayant $n-$ orbites

$$E = \bigcup_{i\in[1,n]} Orb(x_i) \quad \text{(réunion disjointe d'orbites distinctes)}$$

où $x_i \in E$ est un élément (un représentant) de la i-ème orbite. En passant au cardinal:

$$\mid E \mid = \sum_{i\in[1,n]} \mid Orb(x_i) \mid .$$

- Le stabilisateur $Stab_x = \{g \in G, g \cdot x = x\}$ de $x \in E$ est un sous-groupe de G.

- Application d'orbite: $G \to Orb(x) \subset E : g \mapsto g \cdot x$. L'application d'orbite est constante sur les $Stab_x-$ classes à gauche de G et induit un isomorphisme

$$G/Stab_x \to Orb(x) : \overline{g} \mapsto g \cdot x.$$

Corollaire: pour G fini, $\mid G \mid = \mid Orb(x) \mid \cdot \mid Stab_x \mid$.

- Equation des classes: pour l'action de G sur $E = G$ par conjugaison: $G \times G \to G : (g, x) \mapsto gxg^{-1}$, $Orb(x)$ est la classe de conjugaison C_x de x dans G et $Stab_x = \{g \in G, gx = xg\}$ est le centralisateur Z_x de x dans G. Pour G fini, n le nombre de classes de conjugaison et $x_i, i \in [1, n]$, un élément de chaque classe, on a

$$\mid G \mid = \sum_{i\in[1,n]} \mid C_{x_i} \mid = \sum_{i\in[1,n]} \frac{\mid G \mid}{\mid Z_{x_i} \mid}$$

i.e.

$$1 = \sum_{i \in [1,n]} \frac{1}{\mid Z_{x_i} \mid} \quad \text{(Equation des classes)}$$

6) Anneaux et corps

A l'exception de l'anneau $M_n(K)$ des matrices carrées de taille n à coefficients dans un corps commutatif K pour les lois usuelles d'addition et de multiplication matricielles

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}), \quad (a_{ij}) \cdot (b_{ij}) = (\sum_{k=1}^{n} a_{ik} b_{kj}),$$

[$M_n(K)$ est isomorphe à l'anneau $End(K^n)$ des endomorphismes pour les lois d'addition et de composition], tous les anneaux $(A, +_A, \cdot_A)$ considérés dans ce cours sont *commutatifs*, i.e.

$$\forall a, b \in A, \quad a \cdot_A b = b \cdot_A a$$

Dans ce qui suit $(A, +_A, \cdot_A)$ est commutatif et à unité.
Les exemples principaux sont: $Z, Z/nZ$, les corps usuels Z/pZ (p premier), Q, R, C et certains sous-anneaux usuels (par ex. les décimaux dans Q, les entiers de Gauss dans C,...), l'anneau des polynômes en une variable $K[X]$ à coefficients dans un corps commutatif K.

Voici les notions et résultats importants du chapitre:

- Définitions: anneau à unité, corps, produit d'anneaux, idéal, idéal principal (de la forme aA, $a \in A$), morphismes d'anneaux à unité. Le noyau d'un morphisme est un idéal.

- Diviseurs de zéro dans A. Anneau intègre (pas de diviseur de zéro dans A). Anneau principal (tout idéal de A est principal). Anneau euclidien (par ex. Z et la division euclidienne). Groupe des inversibles multiplicatifs $(A^\star, \cdot_A)$.

- Tout anneau euclidien est principal.

- L'anneau des polynômes $K[X]$ en une variable à coefficients dans un corps commutatif K est euclidien. [Savoir effectuer une division de polynômes et/ou calculer un reste. La preuve (par récurrence sur le degré) de l'existence et unicité de cette division n'est pas au prgm du partiel.]

- éléments irréductibles et éléments réductibles de A.

- pour A principal (surtout Z et $K[X]$) pgcd, éléments étrangers, identité de Bézout et lemme de Gauss.

- morphisme d'évaluation: pour $a \in K$, $K[X] \to K : P(X) \mapsto P(a)$.
$(X - a)$ divise $P(X)$ ssi $P(a) = 0$. Tout polynôme $P(X) \in K[X]$ admet au plus degré (P) racines distinctes dans K. Polynômes scindés sur un corps K. Développement de Taylor et racines multiples.

- irréductibilité et racines. Polynômes irréductibles sur C et R. Exemples et contre-exemples sur Q. Savoir factoriser un polynôme sur C, R, Q dans un exemple guidé.

- caractéristique d'un anneau à unité (l'ordre de l'unité 1_A dans le groupe additif $(A, +_A)$).