UNIVERSITÉ DE PARIS 7
Année 2000-2001, DEUG 2ème année
Groupes et arithmétique (MT282)

3 Groupes et anneaux

3.1 Quelques anneaux

Démontrer que les ensembles suivants sont des anneaux.

1. L'ensemble $\mathbf{R}^{\mathbf{N}}$ des suites à valeurs réelles muni de l'addition et de la multiplication des suites.
2. L'ensemble des fonctions continues d'un intervalle réel I dans $\mathbf{R}$ muni de l'addition et de la multiplication des fonctions.
3. L'ensemble des endomorphismes d'un espace vectoriel E muni de l'addition et de la composition des endomorphismes.
4. L'ensemble $\mathbf{Q}[X]$ des polynômes à coefficients rationnels muni de l'addition et de la multiplication des polynômes.
5. L'ensemble des homomorphismes d'un groupe commutatif G dans lui-même, muni de la loi de G (*i.e.* si on note + la loi de G, on considère la loi qui à deux homomorphismes f_1 et f_2 associe l'homomorphisme $g \mapsto f_1(g) + f_2(g)$) et de la composition des homomorphismes

3.2 Quelques homomorphismes d'anneaux

1. Soit $x \in \mathbf{R}$. Démontrer que l'application $f_x : \mathbf{Q}[X] \to \mathbf{R}$ qui à P associe $P(x)$ est un homorphisme d'anneaux. On dit que x est *transcendant* si f_x est un injectif, et que x est *algébrique* sinon. Démontrer que x est algébrique si et seulement si il est racine d'un polynôme non nul à coefficients rationnels.
2. Démontrer que l'application $\mathbf{R}^{\mathbf{N}} \to \mathbf{R}$ qui à $(u_n)_{n\in\mathbf{N}}$ associe u_0 est un homomorphisme d'anneaux.
3. Soit A et B deux anneaux. Trouver une application $f : A \to B$ qui vérifie $f(a+a') = f(a) + f(a')$ et $f(aa') = f(a)f(a')$ (a, $a' \in A$) et qui ne soit pas un homomorphisme d'anneaux.

3.3 Caractéristique d'un anneau

Soit A un anneau commutatif. Soient $a \in A$ et n un entier ≥ 0. On note na la somme de n termes $(a + a + ... + a)$ et $(-n)a$ la somme de n termes $-(a + a + ... + a)$.

1. Démontrer que l'application $f : \mathbf{Z} \to A$ qui à n associe $n1_A$ est un homomorphisme d'anneaux.
2. Démontrer que l'ensemble $\{n \in \mathbf{Z}/f(n) = 0_A\}$ est un sous-groupe de $\mathbf{Z}$. Notons le $n\mathbf{Z}$, avec $n \geq 0$. L'entier n est alors la *caractéristique* de A. Quelle est la caractéristique de $\mathbf{Z}/n\mathbf{Z}$?
3. Supposons que A soit un *anneau intègre*, c'est-à-dire $ab = 0_A$ entraîne $a = 0_A$ ou $b = 0_A$ (a, $b \in A$). Démontrer que la caractéristique de A est un nombre premier ou 0.
4. Si la caractéristique de A est un nombre premier, l'anneau A est-il intègre ?
5. Lorsque la caractéristique de A est un nombre premier p, démontrer qu'on a la formule $(a + b)^p = a^p + b^p$ (cf. feuille d'exercices numéro 2). En déduire alors que l'application $A \to A$ qui à a associe a^p est un homomorphisme d'anneaux.

3.4 Les entiers de Gauss

Considérons l'ensemble $\mathbf{Z}[i] = \{a + ib \in \mathbf{C}/a \in \mathbf{Z}, b \in \mathbf{Z}\}$. C'est l'ensemble des *entiers de Gauss*.

1. Démontrer que $\mathbf{Z}[i]$ muni de l'addition et de la multiplication est un anneau.
2. Démontrer que l'application $a + ib \mapsto a - ib$ est un isomorphisme d'anneaux de $\mathbf{Z}[i]$ dans lui-même.
3. Considérons l'application $N : \mathbf{Z}[i] \to \mathbf{Z}$ qui à $a + ib$ associe $a^2 + b^2 = (a - ib)(a + ib)$. Démontrer qu'on a $N(z)N(z') = N(zz')$ (z, $z' \in \mathbf{Z}[i]$).
4. Soit $z \in \mathbf{Z}[i]^*$. Démontrer qu'on a $N(z) = 1$.
5. Déterminer $\{z \in \mathbf{Z}[i]/N(z) = 1\}$. En déduire $\mathbf{Z}[i]^*$.

3.5 Formules du binôme et de Jacobi

Soit A un anneau.

1. Démontrer que si A est commutatif on a $(a + b)^2 = a^2 + 2ab + b^2$ (a, $b \in A$) (on pourra ensuite montrer la formule du binôme générale).
2. Vérifier sur un exemple que la formule du binôme n'est pas toujours vérifiée lorsque A n'est pas commutatif (on pourra considérer $M_2(\mathbf{R})$).
3. Posons $[a, b] = ab - ba$ (a, $b \in A$). Démontrer la formule de Jacobi : $[a, [b, c]] + [b, [c, a]] + [c, [a, b]] = 0_A$ (a, b, $c \in A$).
4. Soient a, b, $h \in A$ tels qu'on ait $[h, a] = 2a$, $[h, b] = -2b$ et $[a, b] = h$. Établir les formules $[h, a^n] = 2na^n$ et $[h, b^n] = -2nb^n$. En déduire que l'élément $4ab + h^2 - 2h$ commute à a, b et h.

3.6 Nombres décimaux

On appelle *nombre décimal* un nombre rationnel x tel qu'il existe $n \in \mathbf{Z}$ avec $10^n x \in \mathbf{Z}$.

1. Démontrer que l'ensemble D des nombres décimaux est un sous-anneau de $\mathbf{Q}$.
2. Déterminer D^*.

3.7 Éléments nilpotents et unipotents

Soit A un anneau.

1. Soient x et y deux éléments de A qui commutent (*i.e.* on a $xy = yx$). Démontrer qu'on a, pour tout entier $n \geq 1$, $x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + ... + xy^{n-2} + y^{n-1})$.
2. Soit $x \in A$. On dit que x est *nilpotent* s'il existe un entier $n \geq 0$ tel que $x^n = 0_A$. Démontrer que $1_A - x$ est inversible dans ce cas.
3. Soient x et y des éléments nilpotents de A qui commutent. Démontrer que $(x + y)^n$ est donné par la formule du binôme. En déduire que xy et $x + y$ sont nilpotents.
4. Soit $a \in A$. Considérons $f : A \to A$ qui à x associe $ax - xa$. Démontrer que $f^3(x) = 0_A$ lorsque $a^2 = 0_A$ et que $f^5(x) = 0_A$ lorsque $a^3 = 0_A$. Plus généralement, montrer que si a est nilpotent, il existe un entier $k \geq 0$ tel que $f^k(x) = 0_A$ ($x \in A$). On pourra démontrer au préalable la formule $f^k(x) = \sum_{i=0}^{k} (-1)^i C_k^i a^{k-i} x a^i$.
5. Soit $u \in A$. On dit que c'est un élément *unipotent* si $1_A - u$ est nilpotent. Démontrer que si u et v sont des éléments unipotents qui commutent de A, uv est unipotent. Démontrer que tout élément unipotent de A est inversible et a pour inverse un élément unipotent.

3.8 Systèmes de congruences

Déterminer les entiers n vérifiant les systèmes de congruences.

1. $n \equiv 3 \pmod{37}$ et $n \equiv 4 \pmod{52}$.
2. $n \equiv 21 \pmod{12}$ et $n \equiv 12 \pmod{21}$.
3. $n \equiv 2 \pmod{2}$, $n \equiv 3 \pmod{3}$ et $n \equiv 4 \pmod{4}$.

3.9 Classes de congruence inversibles

Établir la liste des classes de congruence inversibles modulo 36 et donner la liste des inverses.

3.10 Fonction d'Euler

1. Calculer $\phi(2000)$ et $\phi(2001)$ où ϕ est la fonction d'Euler.
2. Démontrer que si un nombre premier p divise n (resp. si $p^2|n$) , on a $p-1|\phi(n)$ (resp. $p(p-1)|n$). Déterminer tous les entiers $n > 0$ tels que $\phi(n) \leq 10$.

3.11 Non finitude de l'ensemble des nombres premiers

Supposons qu'il n'existe qu'un nombre fini de nombres premiers. Notons-les p_1, p_2, ..., p_k. Posons alors $n = p_1 p_2 ... p_k$.

1. Soit a un entier différent de 1 et -1. Démontrer que a n'est pas inversible modulo n. En déduire qu'on a $\phi(n) \leq 2$.
2. Donner l'expression de $\phi(n)$ en fonction des nombres premiers p_1, p_2, ..., p_k. Conclure que la finitude de l'ensemble des nombres premiers est une absurdité.

3.12 Automorphismes d'un groupe

Soit G un groupe. Considérons Aut$G$ l'ensemble des automorphismes de G (c'est-à-dire des isomorphismes de G dans lui-même).

1. Démontrer que Aut$G$ muni de la composition des isomorphismes est un groupe.
2. Soit $g \in G$. Considérons l'application $\phi_g : G \to G$ qui à h associe ghg^{-1}. Démontrer que c'est un automorphisme de G, appelé *automorphisme intérieur*.
3. Posons Int$G = \{\phi_g / g \in G\}$. Démontrer que c'est un sous-groupe de Aut$G$.
4. Démontrer que Int$G$ est distingué dans Aut$G$.

3.13 Quelques homomorphismes de groupes

Démontrer que les applications suivantes sont des homomorphismes de groupes. Dire lesquelles d'entre elles sont des isomorphismes.

1. L'application log : $\mathbf{R}_+^* \to \mathbf{R}$ (où $\mathbf{R}_+^*$ est muni de la multiplication et $\mathbf{R}$ de l'addition).
2. L'application déterminant $GL_2(\mathbf{R}) \to \mathbf{R}^*$.
3. L'application $\mathbf{R} \to \mathbf{U} = \{z \in \mathbf{C} / |z| = 1\}$ qui à x associe $e^{2i\pi x}$, où $\mathbf{R}$ et $\mathbf{U}$ sont munis de l'addition et de la multiplication respectivement.

3.14 La notion d'idéal

Soit A un anneau commutatif. Soit I une partie de A distincte de A. On dit que I est un *idéal* de A si $(I,+)$ est un sous-groupe de $(A,+)$ et si on a $xy \in I$ ($x \in A$, $y \in I$).

1. Vérifier que $n\mathbf{Z}$ est un idéal de $\mathbf{Z}$.
2. Démontrer que la relation sur A définie par $x \equiv y \pmod{I}$ si et seulement si $x - y \in I$ est une relation d'équivalence. On note A/I l'ensemble quotient.
3. Démonter que les relations $x \equiv y \pmod{I}$ et $x' \equiv y' \pmod{I}$ entraîne $x + x' \equiv y + y' \pmod{I}$ et $xx' \equiv yy' \pmod{I}$
4. En déduire que l'ensemble quotient A/I est muni d'une structure d'anneau, dite structure *d'anneau quotient*, de telle sorte que l'application canonique $A \to A/I$ est un homomorphisme d'anneaux.

3.15 L'anneau $\hat{\mathbf{Z}}$

Pour n et m deux entiers > 0 tels que $m|n$, on note $\pi_{n,m}$ la surjection canonique $\mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$ qui à $k + n\mathbf{Z}$ associe $k + m\mathbf{Z}$ (où on note $k + n\mathbf{Z}$ la classe de k modulo n). Notons $\hat{\mathbf{Z}}$ l'ensemble des éléments $(u_1, u_2, u_3, ...) \in \mathbf{Z}/\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \times ...$ tels qu'on ait $\pi_{n,m}(u_n) = u_m$ (n, m entiers > 0 avec $m|n$).

1. Démontrer que $\hat{\mathbf{Z}}$ est un anneau (on pourra le voir comme sous-anneau de $\mathbf{Z}/\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \times ...$).
2. Démontrer que l'application $\mathbf{Z} \to \mathbf{Z}/\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \times ...$ qui à k associe $(k + \mathbf{Z}, k + 2\mathbf{Z}, k + 3\mathbf{Z}, ...)$ est à valeurs dans $\hat{\mathbf{Z}}$, puis qu'elle induit un homomorphisme d'anneaux injectif $\iota : \mathbf{Z} \to \hat{\mathbf{Z}}$.
3. Démontrer qu'il existe un élément $(u_1, u_2, u_3, ...) \in \hat{\mathbf{Z}}$ défini par les congruences $u_{2^t m} = 1 + 2^t\mathbf{Z}$ et $u_{2^t m} = 0 + m\mathbf{Z}$ (t entier ≥ 0, m entier impair). Démontrer qu'il n'existe pas $u \in \mathbf{Z}$ tel que $u_n = u + n\mathbf{Z}$ (n entier > 0). L'homomorphisme ι est-il un isomorphisme ?