Algèbre, Master 1 **22 septembre 2008**
2008–2009

TD1 : Groupes, exemples et généralités

Exercice 1 Soit G un ensemble non vide muni d'une loi associative et d'un élément 1 tels que pour tout g de G, $1g = g$ et il existe $h \in G$ tel que $hg = 1$. Montrer que G est un groupe.

Exercice 2 Soit G un groupe. Montrer que

(a) Si H est une partie finie non vide de G telle que pour tout $x, y \in H$ on a $xy \in H$, alors H est un groupe.

(b) Si $\{H_i, i \in I\}$ est une famille de sous-groupes de G, alors $\cap_{i\in I} H_i$ est un sous-groupe de G.

(c) Donner une condition nécessaire et suffisante pour que l'union de deux sous-groupes de G soit un sous-groupe de G.

(d) Si K, H sont deux sous-groupes de G alors $HK = \{hk, h \in H, k \in K\}$ est un sous-groupe de G si et seulement si $HK = KH$.

Exercice 3 (a) Un groupe dont le carré de chaque élément égale le neutre est abélien.

(b) Montrer que l'application $x \to x^{-1}$ est un homomorphisme d'un groupe G si et seulement si G est abélien.

Exercice 4 Montrer qu'un sous-groupe d'indice 2 est toujours distingué.

Exercice 5 Montrer que l'application $a \longmapsto a^{-1}$ est un homomorphisme d'un groupe G si et seulement si G est abélien.

Exercice 6 Soient G un groupe, N un sous-groupe distingué de G et $\pi : G \to G/N$ l'homomorphisme canonique. Démontrer que la correspondance qui associe à chaque sous-groupe L de G/N $\pi^{-1}(L)$ représente une bijection entre les sous-groupes de G/N et les sous-groupes de G contenant N. De plus, cette correspondance preserve les sous-groupes distingués et les indices des sous-groupes.

Exercice 7 Soit G un groupe. Montrer que

(a) Si $G = \mathbb{Z}$ alors tout sous-groupe de G est de la forme $n\mathbb{Z}$, avec n un entier positif. En déduire que si p, q sont premiers entre eux, ils existent des entiers r, s tels que $rp + sq = 1$. Ce résultat est connu comme le théorème de Bezout.

(b) Si $G = \mathbb{Q}^*$ alors G n'est pas de type fini. (Un groupe est de type fini s'il est engendré par un nombre fini des éléments.)

(c) Soit $G = \mathbb{R}$.

(i) Montrer que les sous groupes de $\mathbb{R}$ sont soit monogènes soit denses ;

(ii) Donner un exemple de sous-groupe de $\mathbb{R}$ dense de type fini ;

(iii) Tous les sous-groupes de $\mathbb{R}$ sont-ils de type fini ?

Exercice 8 On désigne par $\mathbb{Z}_n$ le groupe additif des entiers modulo n. (Le groupe $\mathbb{Z}_n$ est aussi identifié avec le groupe additif de l'anneau $\mathbb{Z}/n\mathbb{Z}$.)

(a) Soit d un diviseur de n. Montrer qu'il existe un et un seul sous-groupe C_d de $\mathbb{Z}_n$ d'ordre d.

(b) Montrer que $i(\mod n)$ est un générateur de $\mathbb{Z}_n$ si et seulement si i et n sont premiers entre eux.

(c) (*Fonction indicatrice d'Euler*[1]) On note $\varphi(d)$ le nombre d'entiers entre 1 et d, co-premiers à d.

(i) Montrer que $\phi(d)$ est le nombre de générateurs du sous-groupe C_d de (a).

(ii) Montrer que si $\text{pgcd}(n, m) = 1$ alors $\varphi(nm) = \varphi(n)\varphi(m)$.

(iii) Calculer $\varphi(p^n)$ lorsque p est premier, puis $\varphi(n)$ pour tout entier n.

(iv) Montrer que $n = \sum_{d|n} \varphi(d)$.

(v) Montrer que $\liminf \frac{\varphi(n)}{n} = 0$ et que $\limsup \frac{\varphi(n)}{n} = 1$.

Exercice 9 Soit n un entier strictement positif,

(a) Montrer que $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ engendre $(\mathbb{Z}/n\mathbb{Z}, +) \iff \bar{k}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$.

(b) Montrer que $\text{Aut}(\mathbb{Z}/n\mathbb{Z}, +)$ est isomorphe au groupe des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

(c) Quel est l'ordre des groupes suivants : $\text{Aut}(\mathbb{Z}/p\mathbb{Z}, +)$ (p premier), $\text{Aut}(\text{Aut}(\mathbb{Z}/9\mathbb{Z}))$ et $\text{Aut}(\text{Aut}(\text{Aut}(\mathbb{Z}/9\mathbb{Z})))$?

Exercice 10 Soit K un corps, n un entier > 1 et $e_1, \cdots, e_n$ la base canonique de l'espace vectoriel K^n. On identifie les éléments du groupe $\text{GL}_n(K)$ avec les opérateurs linéaires inversibles de K^n. Pour tous $1 \leq i < j \leq n$ et $t \in K$ on définit $s_{ij}(t) \in \text{GL}_n(K)$ par $s_{ij}(t)e_k = e_k$ si $k \neq j$ et $s_{ij}(t)e_j = te_i + e_j$. (Les opérateurs $s_{ij}(t)$ s'appellent *transvections*.)

(a) Montrer que $\text{SL}_n(K)$ est engendré par des transvections.

[1] Leonhard Euler (1707 Basel, 1783 St-Petersbourg) élève de Jean Bernoulli, il prolongea ses travaux en affinant la notion de fonction dérivée. En 1734 il créa la notion d'équation aux dérivées partielles et en 1744 le calcul des variations : recherche d'extremums sur les surfaces. C'est lui qui fixa les notations aujourd'hui bien connues suivantes : $f(x)$, π, e^x, i et $\sum_{i=1}^{n} x_i$.

(b) On désigne par $\mathrm{U}_n^+(K)$ (respectivement, $\mathrm{U}_n^-(K)$) le groupe des matrice supérieures (respectivement, inférieures) avec 1 sur la diagonale principale. Montrer que $\mathrm{SL}_n(K)$ est engendré par $\mathrm{U}_n^+(K)$ et $\mathrm{U}_n^-(K)$.

(c) Montrer que $\mathrm{GL}_n(K)$ est engendré par $\mathrm{U}_n^+(K)$, $\mathrm{U}_n^-(K)$ et les matrices diagonales $d(t)$ définies par $d(t)e_i = e_i$ et $d(t)e_n = te_n$.

Exercice 11 (a) Soit G un groupe fini d'ordre n tel que pour tout diviseur d de n, il y ait au plus d éléments g de G vérifiant $g^d = 1$. Montrer que G est cyclique.

(b) Montrer que le groupe multiplicatif d'un corps commutatif fini est cyclique. En déduire que $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}, +)$ (p premier) est isomorphe à $\mathbb{Z}_{p-1}$.

Exercice 12 On note $\mathfrak{S}_n$ le groupe des permutations et $\mathfrak{A}_n$ le sous-groupe alterné, de l'ensemble à n éléments $\{1, \cdots, n\}$. Pour $a_1, \cdots, a_k \in \{1, \cdots, n\}$, on note $(a_1, \cdots, a_k)$ la permutation (appelée cycle de longueur k) envoyant a_1 sur a_2,$\cdots$, a_{k-1} sur a_k et fixant chaque $j \notin \{a_1, \cdots, a_k\}$. L'ensemble $\{a_1, \cdots, a_k\}$ est appelé support du cycle.

(a) Montrer que deux cycles de supports disjoints commutent et que toute permutation de $\mathfrak{S}_n$ s'écrit de manière unique (à l'ordre près) comme le produit de cycles de supports disjoints.

(b) Montrer que $\sigma(a_1, \cdots, a_k)\sigma^{-1} = (\sigma(a_1), \cdots, \sigma(a_k))$ pour tout $\sigma \in \mathfrak{S}_n$.

(c) Montrer que les transpositions (i.e. les 2-cycles) engendrent $\mathfrak{S}_n$ et que l'on peut se restreindre à $(1,2), (1,3), \cdots, (1,n)$, ou à $(1,2), (2,3), \cdots, (n-1,n)$. Même question avec $(1,2), (2, \cdots, n)$.

(d) À quelles conditions deux éléments de $\mathfrak{S}_n$ sont-ils conjugués ?

(e) Déterminer les classes de conjugaison de $\mathfrak{S}_3$, de $\mathfrak{S}_4$, de $\mathfrak{S}_5$, de $\mathfrak{A}_3$, de $\mathfrak{A}_4$ et de $\mathfrak{A}_5$.

Exercice 13 (*Symbole de Legendre*[2]) Soit p un nombre premier impair.

(a) Montrez que x est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $x^{\frac{p+1}{2}} = x \mod (p)$. *(On note* $(\frac{x}{p}) = +1$ *ou* -1 *selon que* x *est ou n'est pas un carré mod p. C'est le symbole de Legendre.)*

(b) Trouver une condition nécessaire et suffisante pour que -1 soit un carré modulo p.

(c) Montrez que pour tous $a, b, c \in (\mathbb{Z}/p\mathbb{Z})^*$, l'équation $ax^2 + by^2 = c$ a une solution (x, y) dans $(\mathbb{Z}/p\mathbb{Z})^2$.

(d) Montrez qu'il existe une infinité de nombres premiers congrus à 1 modulo 4 (en est-il de même pour 3 modulo 4).

Exercice 14 (*Structure de* $(\mathbb{Z}/n\mathbb{Z})^*$).

[2] Adrien-Marie Legendre, mathématicien français né le 18 septembre 1752 et mort le 10 janvier 1833 à Paris. Il étudia la théorie des nombres (1778), exposa la méthode des moindres carrés (1806) et établit une classification des intégrales elliptiques (1825).

(a) Soit p un nombre premier ($p \neq 2$), montrer que

$$\forall k \in \mathbb{N}^*, \exists \lambda \in \mathbb{N}^*, \text{ avec } \lambda \wedge p = 1, \text{ et } (1+p)^{p^k} = 1 + \lambda p^{k+1}$$

En déduire que pour tout $n \geqslant 1$ on a $(\mathbb{Z}/p^n\mathbb{Z})^* \cong \mathbb{Z}/p^{n-1}(p-1)\mathbb{Z}$.

(b) En montrant que pour tout $k \geqslant 1$, $5^{2^k} = 1 + \lambda 2^{k+2}$ avec λ un entier impair, déduire pour $n \geqslant 2$ l'isomorphisme

$$(\mathbb{Z}/2^n\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$$

(c) Donner la structure de $(\mathbb{Z}/n\mathbb{Z})^*$. Pour quelles valeurs de n est-il cyclique ?

Exercice 15 Soit $\mathbb{H}_8$ le sous-groupe de $GL_2(\mathbb{C})$ engendré par les matrices

$$I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \; J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \text{ et } K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

(a) Calculez l'ordre de $\mathbb{H}_8$.

(b) Exhibez tous ses sous-groupes, ses sous-groupes distingués, son centre et ses quotients.

(c) En déduire que tous sous groupes de $\mathbb{H}_8$ sont distingués et cycliques.

Exercice 16 Soit p un nombre premier l'ensemble $V_n = (\mathbb{Z}/p\mathbb{Z})^n$ est un espace vectoriel sur le corps $\mathbb{Z}/p\mathbb{Z}$.

(a) Quel est le cardinal de $GL(V_n)$?

(b) Donner un sous-groupe de $GL(V_n)$ d'ordre $p^{\frac{n(n-1)}{2}}$.

(c) Quand $GL(V_n)$ et $GL(V_m)$ sont-ils isomorphes ?

(d) Trouver un homomorphism injectif de $\mathfrak{S}_n$ dans $GL_n(\mathbb{F}_p)$.

Exercice 17 Soit G un groupe, $\mathrm{Aut}(G)$ le groupe des automorphismes de G et $\mathrm{Int}(G)$ l'ensemble des automorphismes intérieurs de G (i.e. l'ensemble des éléments α de $\mathrm{Aut}(G)$ tel qu'il existe un g dans G vérifiant $\forall h \in G$, $\alpha(h) = ghg^{-1}$). Montrer que :

(a) $\mathrm{Int}(G)$ est un sous-distingué de $\mathrm{Aut}(G)$;

(b) $\mathrm{Int}(G) \cong G/Z(G)$, où $Z(G)$ désigne le centre de G ;

(c) Si $\mathrm{Aut}(G)$ est cyclique alors G est abélien ;

(d) Si $|G| > 2$ alors le groupe $\mathrm{Aut}(G)$ ne peut pas être cyclique d'ordre impair.

Exercice 18 Trouver à isomophisme près tous les groupes d'ordre inférieur à 8.

Exercice 19 Soient G un groupe, on dit qu'un sous groupe H de G est maximal si $H \neq G$ et si pour tout sous groupe N de G, $H \subset N \subset G$ implique $N = G$ ou $N = H$.

(a) Les sous groupes maximaux sont-ils nécessairement isomorphes entre eux ?

(b) Montrer que l'intersection de deux sous groupes maximaux commutatifs distincts est incluse dans le centre de G.

(c) Si G est fini, simple et non commutatif alors G contient deux sous groupes maximaux H et H' tels que $H \cap H' \neq \{e\}$ (on utilisera le fait que G ne peut être la réunion des conjugués de H).

(d) Un groupe simple, fini et non commutatif contient un sous groupe maximal non commutatif.