Année universitaire 2011-2012
Master 1 de mathématiques
Algèbre générale de base

Feuille d'exercices 1

Relations d'équivalence

Exercice 1. Dans chacun des cas suivants, dire si la relation d'équivalence $\mathscr{R}$ considérée, sur l'ensemble E, est compatible avec les opérations désignées :

1. $E = \mathbb{R}$; $\mathscr{R} = \{(x, y) \mid |x| = |y|\}$; addition, multiplication.
2. $E = \mathbb{Z}$; $\mathscr{R} = \{(x, y) \mid x = y = 0 \text{ ou } xy > 0\}$; addition, multiplication.
3. $E = \mathbb{Z}$; $\mathscr{R} = \{(x, y) \mid \ x \text{ et } y \text{ sont de même parité}\}$; addition, multiplication.
4. $E = \mathbb{R}$; $\mathscr{R} = \{(x, y) \mid x - y \in \mathbb{Z}\}$; addition, multiplication.
5. $E = \mathbb{N}^*$; $\mathscr{R} = \{(x, y) \mid \ x \text{ et } y \text{ sont de même parité}\}$; puissance.

Révisions sur les groupes

Exercice 2. Soient G un groupe, E un ensemble, $f : E \to G$ une bijection. Montrer qu'il existe une unique structure de groupe sur E telle que f soit un isomorphisme. Expliciter cette loi lorsque $E = \mathbb{Z}$, $G = (\mathbb{Z}, +)$, $f(x) = x + 1$.

Exercice 3. Une propritété P d'un groupe G est *invariante par isomorphie* si, chaque fois que G et G' sont isomorphes, G vérifie P si (et seulement si) G' vérifie P. Parmi les propriétés suivantes, lesquelles sont invariantes par isomorphie ?

1. « G est commutatif » ;
2. « G est fini » ;
3. « G est un sous-groupe de $\mathbb{Z}$ » ;
4. « il existe un morphisme surjectif de $(\mathbb{R}, +)$ dans G » ;
5. « il existe $x \in G$ tel que $x^2 = e_G$ et $x \neq e_G$ ».

Exercice 4. Soit $f : G \to H$ un morphisme de groupes.

1. On suppose H commutatif et f injectif. Montrer que G est commutatif.
2. On suppose G commutatif et f surjectif. Montrer que H est commutatif.
3. Donner des contre-exemples si l'on supprime l'hypothèse sur f.

Exercice 5. Soit H un sous-groupe de $(\mathbb{Z}, +)$. Montrer qu'il existe un unique entier $r \geq 0$ tel que $H = r\mathbb{Z}$.

Exercice 6 (Ordre d'un élément)**.** On rappelle que l'ordre d'un élément g dans un groupe G (dont la loi est notée multiplicativement) est le plus petit entier r strictement positif vérifiant $g^r = e_G$ (et $+\infty$ s'il n'existe aucun r ayant cette propriété).

1. Quel est l'ordre de -1 dans $(\mathbb{Q}, +)$? Et dans $(\mathbb{Q}^*, \times)$?

2. Avec les notations ci-dessus, montrer que l'application $m \mapsto g^m$ est un morphisme de $(\mathbb{Z}, +)$ dans G ; expliquer le lien entre son noyau et l'ordre de g.
3. Soit $f : G \to G'$ un morphisme de groupes, et soit $g \in G$. Montrer que l'ordre de $f(g)$ divise l'ordre de g (on précisera ce qui se passe lorsque l'un des ordres est infini), avec égalité si f est injectif.
4. Soient n un entier ≥ 1 et a un entier. On note $\bar{a}$ la classe de a dans $\mathbb{Z}/n\mathbb{Z}$. Quel est l'ordre de $\bar{a}$ dans le groupe $(\mathbb{Z}/n\mathbb{Z},+)$? (On pourra d'abord considérer le cas simple où a et n sont premiers entre eux.)

Exercice 7 (Groupe des homomorphismes)**.** Soient G et A deux groupes. Notons $\mathrm{Hom}(G, A)$ l'ensemble des homomorphismes de G dans A, et A^G l'ensemble des applications de G dans A.

1. Pour quelle loi interne l'ensemble A^G est-il un groupe ? (Ne pas le démontrer.)
2. Donner une condition suffisante sur A pour que l'ensemble $\mathrm{Hom}(G, A)$ soit un sous-groupe de A^G. Donner un contre-exemple où $\mathrm{Hom}(G, A)$ n'est pas un sous-groupe de A^G.
3. Établir une bijection entre les ensembles A et $\mathrm{Hom}(\mathbb{Z}, A)$. Que dire de cette bijection dans le cas où le groupe A est abélien ?
4. On suppose que A est abélien, et on le note additivement. Soit $n \in \mathbb{N}^*$. Établir un isomorphisme entre $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, A)$ et le sous-groupe suivant de A : $\{x \in A \mid nx = 0\}$.
5. Soient n et m deux entiers ≥ 1. Expliciter le sous-groupe de $\mathbb{Z}/m\mathbb{Z}$ auquel est isomorphe le groupe $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$.

Exercice 8 (Sous-groupes d'indice 2)**.** Soient G un groupe fini et H un sous-groupe d'indice 2 (on rappelle que l'indice est le cardinal de l'ensemble quotient G/H). Montrer que H est distingué.

Exercice 9 (Centre d'un groupe)**.** Soient G un groupe, et $Z = \{h \in G \mid \forall g \in G,\ gh = hg\}$ son *centre*.

1. Montrer que Z est un sous-groupe distingué de G.
2. On suppose que G/Z est cyclique. Montrer que G est abélien.

Exercice 10 (Conjugaison, automorphismes intérieurs)**.** Soient G un groupe.

1. Pour tout $g \in G$, montrer que l'application $\mathrm{int}_g : x \mapsto gxg^{-1}$ est un endomorphisme de G (appelé *conjugaison par* g).
2. Pour tous g et h dans G, montrer que $\mathrm{int}_g \circ \mathrm{int}_h = \mathrm{int}_{gh}$. En déduire que int_g est un automorphisme de G (les automorphismes de cette forme sont dits *intérieurs*) et que l'application $g \mapsto \mathrm{int}_g$ est un morphisme de G dans $\mathrm{Aut}(G)$. Quel est son noyau ?
3. Donner un exemple d'automorphisme non intérieur.

Exercice 11 (Partie génératrice du groupe $\mathrm{SL}_2(\mathbb{Z})$)**.** Soit Γ le sous-groupe de $\mathrm{SL}_2(\mathbb{Z})$ engendré par $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $U = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

1. Soit $M \in \mathrm{M}_2(\mathbb{Z})$. Montrer qu'il existe $A \in \Gamma$ telle que AM soit triangulaire supérieure.

2. Montrer que $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.

Exercice 12 (Le groupe symétrique $\mathfrak{S}_n$ n'est pas résoluble pour $n \geq 5$)**.** Soit G un groupe. Pour a et b dans G, on note $[a, b] = aba^{-1}b^{-1}$. Un tel élément est appelé *commutateur*. On appelle *groupe dérivé* de G, et on note $D(G)$, le sous-groupe de G engendré par les commutateurs. On dit que le groupe G est *résoluble* s'il existe un entier k et des sous-groupes G_0, G_1, …, G_k tels que $G_0 = G$, G_k est le sous-groupe trivial, et $D(G_i) = G_{i+1}$ pour $0 \leq i \leq k-1$. Le but de l'exercice est de montrer que le groupe $\mathfrak{S}_n$ n'est pas résoluble pour $n \geq 5$.

1. Montrer que pour $n \geq 3$, le groupe alterné $\mathfrak{A}_n$ est engendré par les 3-cycles. (On rappelle que le groupe symétrique $\mathfrak{S}_n$ est engendré par les transpositions.)
2. Montrer que tous les cycles de même longueur sont conjugués dans $\mathfrak{S}_n$.
3. Déduire des deux questions précédentes que $D(\mathfrak{S}_n) = \mathfrak{A}_n$ pour $n \geq 2$. (Remarquer que le carré d'un 3-cycle est également un 3-cycle !)
4. Montrer que, pour $n \geq 5$, tous les 3-cycles sont conjugués dans $\mathfrak{A}_n$. En déduire que $D(\mathfrak{A}_n) = \mathfrak{A}_n$ pour $n \geq 5$. Conclure.