Algèbre et arithmétique 4
CONTRÔLE CONTINU N° 1

Exercice 1

Soient G, G' deux groupes finis, et $f : G \to G'$ un morphisme de groupes.
a) Montrez que les cardinaux de $Im(f)$ et $Ker(f)$ divisent les cardinaux de G et G' respectivements.

On sait que $Im(f)$ est un sous-groupe de G et $Ker(f)$ un sous-groupe de G'. Le théorème de Lagrange affirme que le cardinal d'un sous-groupe divise le cardinal du groupe, ce qui conclut.

b) Montrez que $|G| = |Im(f)|\,|Ker(f)|$.

Notons f_1 l'application restreinte à l'arrivée : $f_1 : G \to Im(f)$. Le morphisme f_1 est alors surjectif, et passe au quotient modulo son noyau en une application, encore surjective , $\bar{f_1} : G/Ker(f) \to Im(f)$, qui est aussi injective (car de noyau $Ker(f)/Ker(f)$, qui est trivial). Donc $Im(f)$ est isomorphe à $G/Ker(f)$. Donc leurs cardinaux sont égaux :

$$|Im(f)| = |G/Ker(f)| = |G|/|Ker(f)|,$$

la dernière égalité résultant du cours. D'où l'égalité demandée.
Remarque : ce résultat est à rapprocher du théorème du rang en algèbre linéaire. Les deux résultats coincïdent d'ailleurs lorsque l'on considère des espaces vectoriels de dimension finie sur des corps finis.

Exercice 2

Montrez que l'image d'un groupe monogène par un morphisme de groupe est encore un groupe monogène.

Soit G un groupe monogène, f un morphisme de G vers un autre groupe G'. Soit a un générateur de G, montrons que $f(a)$ génère $Im(f)$. Soit $y \in Im(f)$, il existe $x \in G$ tel que $f(x) = y$. Comme G est monogène, il existe $n \in \mathbb{Z}$ tel que $x = a^n$. Donc $y = f(a)^n$, ce qui conclut.

Exercice 3

Soit G un groupe. On définit une relation binaire $\mathcal{R}$ sur G par :
$g\mathcal{R}g'$ ssi il existe $x \in G$ tel que $g = xg'x^{-1}$.
a) Montrer que $\mathcal{R}$ définit une relation d'équivalence sur G. (On dit alors que g et g' sont *conjugués* lorsqu'ils sont dans la même classe).

Cet exercice est désormais une application directe du cours : la relation proposée n'est rien d'autre que la relation orbitale pour l'action de G sur G par conjugaison. Au moment où l'exercice était posé, la rédaction attendue ressemblait à ce qui suit.

Montrons que $\mathcal{R}$ est réflexive. Soit $g \in G$, $g = ege^{-1}$ donc $g\mathcal{R}g$. Montrons que $\mathcal{R}$ est symétrique. Soient $g, g' \in G$ tels que $g\mathcal{R}g'$, donc il existe $x \in G$ tel que $g = xg'x^{-1}$. On peut réecrire cette relation $x^{-1}gx = g'$, ou encore

$$g' = (x^{-1})g(x^{-1})^{-1},$$

ce qui montre que $g'\mathcal{R}g$. Montrons que $\mathcal{R}$ est transitive, soient g, g', g'' tels que $g\mathcal{R}g'$ et $g'\mathcal{R}g''$ donc il existe x, y tels que $g = xg'x^{-1}$ et $g' = yg''y^{-1}$, donc

$$g = xyg''y^{-1}x^{-1} = (xy)g''(xy)^{-1},$$

c'est à dire $g\mathcal{R}g''$.

b) Soit H un sous-groupe de G, que l'on suppose distingué, et $f : G \to \{0, 1\}$ la fonction indicatrice de l'ensemble H, càd $f(x) = 1$ si $x \in H$ et $f(x) = 0$ sinon. Montrez que f passe au quotient modulo $\mathcal{R}$, càd se factorise en une application $\bar{f} : G/\mathcal{R} \to \{0, 1\}$.

On sait, d'après le critère de passage au quotient, qu'il nous suffit de vérifier que si $g\mathcal{R}g'$, alors $f(g) = f(g')$. Soient donc g, g' conjugués, il existe x tel que $g = xg'x^{-1}$. Si g' est dans H, alors g aussi car H est distingué, et comme la relation est symétrique, g et g' sont tous deux dans H ou bien tous deux dans le complémentaire de H. Donc $f(g) = f(g')$.

c) Soit $x \in G$. Montrez que $c_x : G \to G$, défini par $c_x(g) = xgx^{-1}$ est un morphisme de groupe, puis que c'est un isomorphisme.

Soient $g, g' \in G$,

$$c_x(g)c_x(g') = xgx^{-1}xg'x^{-1} = x(gg')x^{-1} = c_x(gg'),$$

et donc c_x est un morphisme. On vérifie facilement que $c_x \circ c_{x^{-1}} = Id_G$, et que $c_{x^{-1}} \circ c_x = Id_G$, et donc c_x est bijective. C'est donc un isomorphisme.

d) Soient g, g' deux éléments conjugués. Montrez que les sous-groupes engendrés par g et g' respectivement sont isomorphes. (on pourra s'inspirer des morphismes c_x).

Soit x tel que $g = xg'x^{-1} = c_x(g')$. On a pour tout entier relatif n, $c_x(g'^n) = g^n$ et donc l'image par c_x du sous-groupe engendré par g' (qui est simplement $\langle g' \rangle = \{g'^n : n \in \mathbb{Z}\}$) est le sous-groupe engendré par g. Comme c_x est injective sur G, elle l'est encore en restriction à $\langle g' \rangle$, et donc sa restriction à $\langle g' \rangle$ est un isomorphisme vers $\langle g \rangle$.

e) Montrez que $o : G \to \mathbb{N}$, qui à un élément g associe son ordre, passe au quotient modulo $\mathcal{R}$.

Soit g, g' dans la même classe de conjugaison. D'après la question précédente, les groupes engendrés par g et g' sont isomorphes, donc en particulier ont même cardinal. Ce cardinal étant par définition l'ordre de g et g', on a bien $o(g) = o(g')$. Le critère de passage au quotient est donc satisfait.