Théorie des groupes

Corrigé feuille 5

Exercice 1 On note π le morphisme défini par la projection naturelle sur le quotient : $\pi : G \to G/H$.
$|G/H| = n$ donc $\pi(x)^n = e$, ce qui signifie que $x^n \in \ker \pi = H$.

Exercice 2

1. Soit $a \notin H$. Si il existe $h \in H$ tel que $ah \in H$, alors $a \in H$, ce qui est absurde. Donc $aH \cap H = \emptyset$. De même $H \cap aH = \emptyset$. Par cardinalité, on a donc $aH = Ha$ et $H \lhd G$.
2. G/H est un groupe d'ordre 2, donc est isomorphe (via un morphisme ψ) à $\mathbb{Z}/2\mathbb{Z}$. On note $\varphi : \mathbb{Z}/2\mathbb{Z} \to (\mathbb{C}^*, .)$ le morphisme injectif tel que $\varphi(0) = 1$ et $\varphi(1) = -1$. Alors, $\varphi \circ \psi \circ \pi$ est un morphisme non-trivial de S_n dans $\mathbb{C}^*$. C'est donc la signature. D'où $H = \ker \pi = \ker \varphi \circ \psi \circ \pi = A_n$.

Exercice 3 $K = \{(h, e) \mid h \in H\}$ est toujours propre et distingué.
$\alpha(e) = Id_H$, donc K est isomorphe à H, donc est bien un sous-groupe propre.
Soient $(h_1, g_1) \in H \rtimes_\alpha G$, et $(h, e) \in K$.
$(h_1, g_1)(h, e)(h_1, g_1)^{-1} = (h_1\alpha(g_1)(h)\alpha(g_1)(\alpha(g_1^{-1})(h^{-1})), e) \in K$. Donc $K \lhd H \rtimes_\alpha G$.

Exercice 4

1. Non, exemple : $\varphi : \begin{array}{ccc} \{e, (12)\} & \to & S_3 \\ x & \mapsto & x \end{array}$.
2. L'image d'un sous-groupe distingué n'est pas distinguée. Même exemple que ci-dessus.
   L'image réciproque est distinguée. Soit $H \lhd G$ et $\psi : K \to G$. Soit $x \in \psi^{-1}(H)$, $y \in K$. On note $h = \psi(x)$ et $g = \psi(y)$. Alors $yxy^{-1} = \psi^{-1}(g)\psi^{-1}(h)\psi^{-1}(g^{-1}) = \psi^{-1}(ghg^{-1})$. Comme H est distingué dans G, $ghg^{-1} \in H$, et donc $yxy^{-1} \in \varphi^{-1}(H)$.
3. $\ker det = \mathrm{SL}_n(\mathbb{R}) \lhd \mathrm{GL}_n(\mathbb{R})$. Le quotient est $\mathbb{R}*$.
   Pas distingué : $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$ n'est pas dans $\mathrm{O}_n(\mathbb{R})$
   $\mathrm{SO}_n(\mathbb{R}) \lhd \mathrm{O}_n(\mathbb{R})$ Le quotient est $\mathbb{Z}/2\mathbb{Z}$.

Exercice 5 (Sous-groupes caractéristiques) Soit G un groupe. Un sous-groupe H de G est dit *caractéristique* si pour tout $\alpha \in \mathrm{Aut}(G)$, on a $\alpha(H) = H$. Cela est noté $H \blacktriangleleft G$.

1. $Int(G) \subset Aut(G)$.
2. Soit $g \in Aut(G)$. On sait que $g(H) = H$. Donc $h = g\mid_H$ est dans $Aut(H)$. $h(K) = K$, donc $g(K) = K$.
3. Soit $g \in G$. Pour tout $h \in H$, $ghg^{-1} \in H$, $\varphi_g \in Aut(H)$ Donc $\varphi_g(K) = K$ est $K \lhd G$.

Exercice 6

1. Pour tout , $x, y \in G$, pour tout $\alpha \in Aut(G)$,

$$\alpha(xyx^{-1}y^{-1}) = \alpha(x)\alpha(y)\alpha(x)^{-1}\alpha(y)^{-1} \in D(G)$$

   Donc $\alpha(D(G)) \subset D(G)$. Vrai aussi pour α^{-1} d'où $D(G) \subset \alpha(D(G))$.
2. Soient $\hat{x}$ et $\hat{y}$ dans $G/D(G)$.
   Alors $[\hat{x}, \hat{y}] = \hat{[x, y]}$. $[x, y] \in D(G)$ donc $\hat{[x, y]} = e$, ce qui veut dire que $\hat{x}$ et $\hat{y}$ commutent.
3. Soient x et y dans G. $\hat{[x, y]} = [\hat{x}, \hat{y}] = e$ car G/H abélien. Donc $[x, y] \in H$. En passant au groupe engendré, on en déduit $D(G) \subset H$.

Exercice 7 Lemme :

Soit $\tau = (i_1 \dots i_k)$ un k-cycle de $\mathfrak{S}_n$, et $\sigma \in \mathfrak{S}_n$. Alors :

$$\sigma\tau\sigma^{-1} = (\sigma(i_1) \dots \sigma(i_k))$$

Preuve : On pose $\gamma = (\sigma(i_1) \dots \sigma(i_k))$ et $A = \sigma(Supp\tau) = \{\sigma(i_1) \dots \sigma(i_k)\} = Supp(\gamma)$

Si $x \in A$, il existe un l tel que $x = \sigma(i_l)$.

$\sigma\tau\sigma^{-1}(x) = \sigma\tau\sigma^{-1}(\sigma(i_l)) = \sigma\tau(i_l) = \sigma(i_{l+1}) = \gamma(\sigma(i_l)) = \gamma(x)$.

Si $x \notin A$. Alors $\sigma^{-1}(x) \notin Supp\tau$, c'est à dire $\tau(\sigma^{-1}(x)) = \sigma^{-1}(x)$. Et donc $\sigma\tau\sigma^{-1}(x) = x$. Comme $x \notin A$, x n'est pas dans $Supp\gamma$, et donc $\gamma(x) = x = \sigma\tau\sigma^{-1}(x)$.

On a donc montré que $\sigma\tau\sigma^{-1}$ et γ coïncident en tout point de $[\![1, n]\!]$.

□

K est d'ordre 4 donc est abélien donc $H \lhd K$.

Si $\sigma \in S_4$ et $\{i, j, k, l\} = [\![1, 4]\!]$, alors :

$$\sigma(ij)(kl)\sigma^{-1} = \sigma(ij)\sigma\sigma^{-1}(kl)\sigma^{-1} = (\sigma(i)\sigma(j))(\sigma(k)\sigma(l)).$$

D'où $K \lhd S_4$.

$(13)(12)(34)(13) = (23)(14)$ donc $H \not\lhd S_4$.

Exercice 8 (Sous-groupes maximaux)

1. Soit p premier. Si $p\mathbb{Z} \subset n\mathbb{Z}.$, on a que $n \mid p$, donc $n = \pm 1$ ou $\pm p$ donc $n\mathbb{Z} = \mathbb{Z}$ ou $p\mathbb{Z}$.

   Réciproquement, si $H = n\mathbb{Z}$ est maximal. Si n n'est pas premier, alors $n = pr$ avec p premier et $r \geq 2$. Alors $H \subset p\mathbb{Z}$ et $H \neq p\mathbb{Z}$. Donc H n'est pas maximal. Absurde. Donc p est premier.

2. Soit H un sous-groupe de G. Si H n'est pas maximal, alors il est strictement contenu dans H_1 de cardinal strictement supérieur. On construit ainsi de proche en proche une suite strictement croissante $(H_n)_n$ de sous-groupes emboités. Comme G est fini, ce processus s'arrête forcément à un certain rang k. H_k est alors un sous-groupe maximal contenant H.

3. Soit H distingué dans G, notons π la projection canonique sur G/H. On va montrer un résultat équivalent : H maximal $\Leftrightarrow \frac{G}{H}$ n'a pas de sous-groupe propre. (Voir exercice 3 feuille 4)

   Si H est maximal. Soit K un sous-groupe de G/H. Alors $\pi^{-1}(K)$ est un sous-groupe de G contenant H. Par maximalisé, soit $\pi^{-1}(K) = H$ et alors $K = \{e\}$, soit $\pi^{-1}(K) = G$ et alors $K = G/H$. Donc K n'est pas un sous-groupe propre.

   Si G/H n'a pas de sous-groupe propre. Soit K sous-groupe de G tel que $H \subset K$. Alors $\pi(K)$ est un sous-groupe de G/H. Soit c'est G/H et alors $K = G$, soit c'est $\{e\}$ et alors $K = H$. Donc H est maximal.

Exercice 9 (Automorphismes de $(\mathbb{F}_p)^n$)

1. Soit $\varphi : \begin{array}{ccc} Aut(\mathbb{Z}/p\mathbb{Z}) & \to & (\mathbb{F}_p^\times, \times) \\ \alpha & \mapsto & \alpha(1) \end{array}$.

   $\alpha(1)$ est de même ordre que 1 donc ne peut-être 0 et : $varphi$ est bien définie.

   $\varphi(\alpha\beta) = \alpha \circ \beta(1) = \alpha(1)\beta(1) = \varphi(\alpha)\varphi(\beta)$, donc φ est un morphisme.

   Si $\varphi(\alpha) = 1$, alors pour tout $x \in \mathbb{Z}/p\mathbb{Z}$, $\alpha(x) = x$. Donc $\ker\varphi = \{Id\}$. φ injective

   Pour tout $a \in \mathbb{Z}/p\mathbb{Z}$ non nul, $x \mapsto a.x$ est un automorphisme (car abélien). φ surjective.

   Donc φ isomorphisme.

2. Soit ψ un endomorphisme de $\mathbb{F}_p^n$.

   Soit $\overline{k} \in \mathbb{F}_p$ et k un de ses représentants dans $\mathbb{Z}$. Pour tout $x = (x_1, \dots, x_n) \in \mathbb{F}_p^n$, on a :

   $\psi(\overline{k}x) = \psi(x + x + \dots + x)$ avec k occurrences de x. $\psi(\overline{k}x) = \psi(x) + \psi(x) + \dots + \psi(x) = k\psi(x)$.

   $k\psi(x)$ est indépendant du représentant k choisi, car tous les représentants diffèrent d'un multiple de p et tout élément de $\mathbb{F}_p^n$ est d'ordre divisant p.

   Donc $\psi(\overline{k}x) = \overline{k}\psi(x)$, et ψ est $\mathbb{F}_p$-linéaire.

3. Une base de $\mathbb{F}_p^n$ est constitué de n vecteurs. Notons-la $(e_1, e_2, \dots, e_n)$.

   e_1 peut être n'importe quel élément non nul de $\mathbb{F}_p^n$, ce qui donne $p^n - 1$ éléments possibles.

Une fois e_1 choisi, e_2 peut-être n'importe quel élément qui n'est pas un multiple de e_1. e_1 étant d'ordre p, cela donne $p^n - p$ possibilités pour e_2.

$\vdots$

Une fois les k premiers éléments choisis, le $k+1$-ème peut être n'importe quel élément qui n'est pas une combinaison linéaire des k premiers. Comme $\mathbb{F}_p^n$ est abélien, $Vect(e_1, \ldots, e_k)$ est de cardinal p^k. Ce qui donne $p^n - p^k$ possibilités pour e_{k+1}.

Et ainsi de suite jusqu'à choisir e_n (pour lequel il y a $p^n - p^{n-1}$ choix.

Soit un total de $(p^n-1)(p^n-p)...(p^n-p^{n-1})$ bases de $(\mathbb{F}_p)^n$.

4. On a montré que tout morphisme de groupe est une application linéaire. Réciproquement, toute application linéaire est un morphisme de groupe.

   Donc l'ensemble des automorphismes de $\mathbb{F}_p^n$ est l'ensemble des applications $\mathbb{F}_p^n$-linéaires inversibles.

   A chaque base B de $\mathbb{F}_p^n$ correspond une unique application linéaire inversible qui envoie la base canonique sur B.

   Réciproquement, une application linéaire inversible envoie la base canonique sur une unique base.

   Il y a donc autant d'automorphismes de $\mathbb{F}_p^n$ que de bases de $\mathbb{F}_p^n$, soit $\prod_{i=0}^{n-1}(p^n - p^i)$.

Exercice 10 $\mathcal{A}_1$ et $\mathcal{A}_2$ ne sont pas simples, car réduits à l'élément neutre.

$\mathcal{A}_3$ est d'ordre 2 donc cyclique et donc simple. $\mathcal{A}_4$ n'est pas simple, car le groupe de Klein engendré par les doubles transpositions est distingué dans $\mathcal{A}_4$.

Exercice 11 (Groupe des quaternions)

1. Calcul matriciel, pas de difficulté.
2. Vérifier que tous les éléments sont distincts. Stabilité par produit et inverse par la formule au dessus.
   Pas abélien car $IJ = K = -JI$.
3. $\mathcal{Q}_8$ et $< 1 >$ sont bien sur distingués. Raisonner sur l'ordre des éléments : Q_8 contient un élément d'ordre 1 (1), un élément d'ordre 2, (-1) et 6 éléments d'ordre 4 $(I, -I, J, -J, K, -K)$. Soit H un sous-groupe propre de Q_8.
   Si H contient un élément d'ordre 4, alors il est d'indice 2 donc est distingué. Sinon, comme il n'y a qu'un élément d'ordre 2, $H = \{1, -1\}$. Alors $H = Z(\mathcal{Q}_8)$ et est distingué.
4. Si Q_8 était le produit direct de deux groupes plus petits, il s'agirait de deux groupes d'ordre 2 et 4. Or tous les groupe de ces ordres sont abéliens donc le produit direct serait aussi abélien, ce qui est absurde.
5. Supposons que $Q_8 = G \rtimes_\phi H$ via un morphisme $\phi : H \to \mathrm{Aut}(G)$. Il y a deux possibilités :
   — Soit G est d'ordre 2 et H est d'ordre 4. Alors $\mathrm{Aut}(G)$ est le groupe réduit à l'identité. Et donc $\phi(h) = Id$ pour tout $h \in H$, ce qui signifie que le produit est en fait direct. Absurde.
   — Soit G est d'ordre 4 et H est d'ordre 2. Dans ce cas, on note f l'élément non-trivial de H et on pose $K = \{(e_G, e_H), (e_G, f)\}$.
   K est un sous-groupe de Q_8, car pour tout $x \in H$, $\phi(x)(e_G) = e_G$.
   Or, le seul sous-groupe d'ordre 2 de Q_8 est son centre. (Car il y a autant de sous-groupes d'ordre 2 que d'éléments d'ordre 2 et seul -1 est d'ordre 2). Donc les éléments de K commutent avec tous les autres.
   Soient $g, g' \in G$.
   $(e, f) \star_\phi (g', e) = (\phi(f)(g'), f)$.
   $(g', e) \star_\phi (e, f) = (g', f)$ (car G d'ordre 4 donc abélien).
   Comme (e, f) et (g', e) commutent, on a forcément $\phi(f)(g') = g'$, c'est à dire que $\phi(f)$ est l'identité.
   Comme $\phi(e)$ est toujours l'identité, on en déduit que ϕ est le morphisme trivial envoyant tout élément de H sur l'identité.
   Le produit semi-direct est en fait direct, ce qui est absurde.