Ecole Normale Supérieure Paris Année 2013-2014
Algèbre 1

Corrigé de la Feuille d'exercices 4

Exercice 4

1. On a $N \lhd G$ et $N < K$ donc $N \lhd K$.
2. On a $H < G$ et $K < G$ donc $H \cap K < K$.
3. On a $N \cap H = \{e\}$ donc $N \cap K \cap H = \{e\}$.
4. On a $NH = G$ donc si $k \in K$ alors $k = nh$ avec $n \in N$ et $h \in H$. Puisque $N \subset K$, on déduit que $h \in H \cap K$. D'où $N(H \cap K) = K$.

On déduit que $K = N \rtimes (K \cap H)$.
Exercice 5 Un premier scindage consiste à utiliser le morphisme $x \mapsto \mathrm{Diag}(x, 1, \ldots, 1)$. On trouve que $\mathrm{GL}_n(k) \simeq \mathrm{SL}_n(k) \rtimes k^\times$ où l'on voit $k^\times$ comme le sous-groupe de $\mathrm{GL}_n(k)$ formé des matrices de la forme $\mathrm{Diag}(x, 1, \ldots, 1)$, $x \in k^\times$.
Si $x \mapsto x^n$ est un automorphisme, notons $a : k^\times \to k\times$ son inverse. Alors l'application

$$\begin{array}{rcl} \alpha : \mathrm{SL}_n(k) \times k^\times & \simeq & \mathrm{GL}_n(k) \\ (A,t) & \mapsto & A\mathrm{Diag}(a(t), \ldots, a(t)) \end{array}$$

est un isomorphisme.
Réciproquement, supposons qu'il existe

$$\begin{array}{rcl} \alpha : \mathrm{SL}_n(k) \times k^\times & \simeq & \mathrm{GL}_n(k) \\ (A,t) & \mapsto & \phi(A)s(t) \end{array}$$

un isomorphisme de groupes. Le commutateur de $\mathrm{SL}_n(k) \times k^\times$ est $\mathrm{SL}_n(k)$ et le commutateur de $\mathrm{GL}_n(k)$ est aussi $\mathrm{SL}_n(k)$[1]. On déduit que ϕ est un automorphisme de $\mathrm{SL}_n(k)$. D'un autre côté, $k^\times$ commute avec tout élément de $\mathrm{GL}_n(k)$ et est donc composé uniquement d'homothéties (le centre de $\mathrm{GL}_n(k)$ est formé des homothéties). On a donc que $t \mapsto s(t)$ est un morphisme injectif de la forme $t \mapsto \mathrm{Diag}(a(x), a(x), \ldots, a(x))$ de $k^\times$ vers $\mathrm{GL}_n(k)$.
Puisque le noyau de det est $\mathrm{SL}_n(k)$, on déduit que $a(t)^n = 1$ si, et seulement si, $a(t) = 1$. Donc le morphisme $x \mapsto x^n$ est injectif sur $\mathrm{im}(a)$. Puisque $t \mapsto a(t)$ est injectif on déduit

[1] Sauf dans le cas $n = 2$ et $k = \mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z}$.On peut vérifier dans ces cas l'exo à la main (le cas $k = \mathbb{Z}/2\mathbb{Z}$ on a un produit direct et le cas $k = \mathbb{Z}/3\mathbb{Z}$ ce n'est pas un produit direct.

que $t \mapsto a(t)^n$ est injectif. Or det est surjectif sur $k^\times$. On déduit que $t \mapsto a(t)^n = a(t^n)$ est surjectif, et donc $x \mapsto x^n$ est surjectif et donc un automorphisme.

Exercice 6 Soit G un groupe d'ordre $255 = 3 \cdot 5 \cdot 17$. D'après les théorèmes de Sylow, le nombre n_3 de 3-Sylows vaut 1 ou 85, le nombre n_5 de 5-Sylows vaut 1 ou 51 et on n'a qu'un seul 17-Sylow. On ne peut pas avoir $n_3 = 85$ et $n_5 = 51$ car on aurait trop d'éléments dans G. Donc $n_3 = 1$ ou $n_5 = 1$. Supposons $n_3 = 1$ (l'autre cas se résout de la même façon). Notons S_3 le seul 3-Sylow, S_{17} le seul 17-Sylow et S_5 un 5-Sylow quelconque. On a :

1. $S_3S_{17} \simeq S_3 \times S_{17} \lhd G$.
2. $S_3S_{17} \cap S_5 = \{e\}$.
3. $S_3S_{17}S_5 = G$

On déduit que $G = S_3S_{17} \rtimes S_5$. Soit $\phi : S_5 \to \mathrm{Aut}(S_3S_{17})$ le morphisme correspondant. On sait que $\mathrm{Aut}(S_3S_{17}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$ donc ϕ est trivial et le produit semi-direct est direct.

Exercice 7

1. Le morphisme $\begin{array}{ccc} N \rtimes_\psi H & \to & N \rtimes_\phi H \\ (n,h) & \mapsto & (n, \alpha(h)) \end{array}$ est un isomorphisme.
2. Le morphisme $\begin{array}{ccc} N \rtimes_\psi H & \to & N \rtimes_\phi H \\ (n,h) & \mapsto & (u(n), h) \end{array}$ est l'isomorphisme recherché.
3. H est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et $\mathrm{im}(\phi) = \mathrm{im}(\psi)$ est isomorphe à $\mathbb{Z}/m\mathbb{Z}$ avec m diviseur de n. Il existe donc d premier à m tel que $\phi(1) = d\psi(1)$ dans $\mathbb{Z}/m\mathbb{Z}$. Puisque l'application $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times$ est surjective, il existe $d' \in (\mathbb{Z}/n\mathbb{Z})^\times$ qui s'envoie vers d.

   La multiplication par d' est un automorphisme α de $\mathbb{Z}/n\mathbb{Z}$ qui satisfait aux conditions de (1), d'où le résultat.

Exercice 8

1. Soit G un groupe d'ordre pq. Par lemme de Cauchy (ou théorème de Sylow), il possède un sous-groupe G_p d'ordre p et un sous-groupe G_q d'ordre q. Comme on a $p \wedge q = 1$, l'intersection de G_p et G_q est réduite au neutre; de plus ils engendrent G. Par le lemme d'Ore, G_q est normal dans G et G est donc égal à un produit semi-direct (éventuellement direct) $G_q \rtimes G_p$. Ce produit semi-direct est déterminé par un morphisme $G_p \to \mathrm{Aut}\, G_q$. Autrement dit, on est amené à classifier les morphismes $\mathbb{Z}/p\mathbb{Z} \to (\mathbb{Z}/q\mathbb{Z})^\times \simeq \mathbb{Z}/(q-1)\mathbb{Z}$.
   Si q n'est pas congru à 1 modulo p, un tel morphisme est nécessairement trivial, et

le seul groupe d'ordre pq est alors le produit direct $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \simeq \mathbb{Z}/pq\mathbb{Z}$.
Si q est congru à 1 modulo p, un morphisme $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/(q-1)\mathbb{Z}$ existe et est injectif. De plus, si φ et ψ sont deux tels morphismes, il existe $\alpha \in \operatorname{Aut} \mathbb{Z}/p\mathbb{Z}$ tel que l'on ait $\varphi = \psi \circ \alpha$. Le (1) de l'exercice précédent montre qu'alors on a $\mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/q\mathbb{Z} \rtimes_\psi \mathbb{Z}/p\mathbb{Z}$. Il en résulte qu'il y a dans ce cas-là, à isomorphisme près, deux groupes d'ordre pq: $\mathbb{Z}/pq\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$.

2. Comme q est congru à 1 modulo 2, on a l'existence de deux groupes d'ordre $2q$: le groupe cyclique $\mathbb{Z}/2q\mathbb{Z}$ et un produit semi-direct $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. Ce dernier est bien isomorphe au groupe diédral D_q: il suffit d'identifier $(1,0)$ à une rotation d'ordre maximal et $(0,1)$ à une symétrie.

Exercice 9

1. Soit G un groupe d'ordre 8. Si G possède un élément d'ordre 8, alors G est cyclique, isomorphe à $\mathbb{Z}/8\mathbb{Z}$. Si G est d'exposant 2, alors G est abélien et isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$. Si G est d'exposant 4 et est abélien, alors G est isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Supposons maintenant G d'exposant 4 et non abélien. Soit r un élément d'ordre 4; il engendre un sous-groupe R isomorphe à $\mathbb{Z}/4\mathbb{Z}$. Soit s un élément de $G \setminus \{1, r, r^2, r^3\}$ d'ordre minimal. S'il est d'ordre 2, alors le sous-groupe engendré $S = \{1, s\}$ intersecte R trivialement. Et G est engendré par R et S (puisque ces derniers contiennent au moins 5 éléments). De plus, R est normal par lemme d'Ore et G est isomorphe au produit semi-direct $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \simeq D_4$.
Si s est d'ordre 4, on va renommer r et s respectivement par i et j. Reste à établir la table de G et voir qu'elle coïncide avec celle de $\mathfrak{H}_8$.

2. Supposons $\mathfrak{H}_8 = N \rtimes H$ de manière non triviale. Alors l'un des sous-groupes N ou H est d'ordre 2, donc est exactement $\{\pm 1\}$. Si c'était H, H serait normal et le produit semi-direct serait direct. Comme tout groupe d'ordre 4 est abélien, $\mathfrak{H}_8$ serait abélien, ce qui n'est pas le cas. On peut donc supposer $N = \{\pm 1\}$. Mais alors $\operatorname{Aut} N$ est réduit à un élément et tout morphisme $H \to \operatorname{Aut} N$ est trivial. Le produit semi-direct serait encore direct et $\mathfrak{H}_8$ à nouveau abélien. C'est donc que l'hypothèse initiale est fausse.

3. En passant en revue les éléments de $\mathrm{SL}_2(\mathbb{F}_3)$, il y en a uniquement 8 d'ordre une puissance de 2. Ce sont:

- ordre 1 : $\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$;
- ordre 2 : $\begin{pmatrix} 2 & \\ & 2 \end{pmatrix}$;

- ordre 4 : $\begin{pmatrix} & 1 \\ 2 & \end{pmatrix}$, $\begin{pmatrix} & 2 \\ 1 & \end{pmatrix}$, $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$, $\begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}$
  . Il y a donc un unique 2-Sylow, et il est clairement isomorphe à $\mathfrak{H}_8$.

Exercice 10

1. Les p-Sylow de $\mathrm{GL}_2(\mathbb{F}_p)$ sont d'ordre p. Soit S l'ensemble des p-Sylow de $\mathrm{GL}_2(\mathbb{F}_p)$. Comme le sous-groupe U des matrices unipotentes supérieures est un p-Sylow de $\mathrm{GL}_2(\mathbb{F}_p)$, en faisant agir $\mathrm{GL}_2(\mathbb{F}_p)$ sur S par conjugaison, on voit que S est isomorphe à $\mathrm{GL}_2(\mathbb{F}_p)/\operatorname{Stab} U = \mathrm{GL}_2(\mathbb{F}_p)/B$, où B désigne le Borel standard de $\mathrm{GL}_2(\mathbb{F}_p)$. Cela donne directement la liste à la fin de (1').

1'. Les p-Sylow de $\mathrm{GL}_2(\mathbb{F}_p)$ sont d'ordre p. Comme le sous-groupe U des matrices unipotentes supérieures est un p-Sylow de $\mathrm{GL}_2(\mathbb{F}_p)$ et que tous sont conjugués, on voit qu'une matrice de $\mathrm{GL}_2(\mathbb{F}_p)$ est dans un p-Sylow si et seulement si son polynôme caractéristique est $(X-1)^2$. On dénombre (à la main!) p^2 telles matrices et donc $(p+1)$ p-Sylow distincts (car deux p-Sylow distincts ne s'intersectent qu'en l'élément neutre). On remarque que ce sont les conjugués de U par les $\begin{pmatrix} 1 & \\ a & 1 \end{pmatrix}$, $a \in \mathbb{F}_p$, et $\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$.

2. Comme les images de ψ et φ sont des p-Sylow de $\mathrm{GL}_2(\mathbb{F}_p)$, ils sont conjugués par une matrice $P \in \mathrm{GL}_2(\mathbb{F}_p)$. Notons $\begin{array}{rccc} \varphi^{(P)} : & \mathbb{Z}/p\mathbb{Z} & \to & \psi(\mathbb{Z}/p\mathbb{Z}) \\ & x & \mapsto & P\varphi(x)P^{-1} \end{array}$; c'est un isomorphisme. Dès lors, $(\varphi^{(P)})^{-1} \circ \psi$ est un automorphisme de $\mathbb{Z}/p\mathbb{Z}$, donc donné par un $x \mapsto kx$ pour un certain $k \in \mathbb{Z}$ premier avec p.

3. Comme on a $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \simeq \mathrm{GL}_2(\mathbb{F}_p)$, la question 1 nous donne l'existence d'un tel produit semi-direct non trivial. L'unicité découle de 2 et de l'exercice 7.

4. Comme le centre d'un p-groupe est non trivial, le centre de $(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes \mathbb{Z}/p\mathbb{Z}$, ne peut être que d'ordre p, p^2 ou p^3. Mais s'il était d'ordre p^2 ou p^3, l'exercice 8 (TD1) nous dirait que $(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes \mathbb{Z}/p\mathbb{Z}$ est abélien. Ce n'est pas le cas, et donc le centre est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

5. La suite exacte suivante est scindée.
$$1 \to \begin{pmatrix} 1 & & \mathbb{F}_p \\ & 1 & \mathbb{F}_p \\ & & 1 \end{pmatrix} \to \begin{pmatrix} 1 & \mathbb{F}_p & \mathbb{F}_p \\ & 1 & \mathbb{F}_p \\ & & 1 \end{pmatrix} \to \begin{pmatrix} 1 & \mathbb{F}_p & \\ & 1 & \\ & & 1 \end{pmatrix} \to 1$$
Le centre du groupe unipotent supérieur s'identifie alors à $\begin{pmatrix} 1 & & \mathbb{F}_p \\ & 1 & \\ & & 1 \end{pmatrix}$.