+1/1/60+

EPFL

1

Teacher : Dimitri Wyss
Structures algébriques - MA
25.01.2024
Duration : 180 minutes

Student 1

SCIPER : **999000** Signature :

Do not turn the page before the start of the exam. This document is double-sided, has 4 pages, the last ones possibly blank. Do not unstaple.

- Place your student card on your table.
- **No other paper materials** are allowed to be used during the exam.
- Using a **calculator** or any electronic device is not permitted during the exam.
- The space allotted is sufficient, so do not add a sheet to your exam. Page 4 is empty. If necessary, specify at the end of the exercise that you are continuing on page 4 (otherwise the page will not be corrected).
- Use a **black or dark blue ballpen** and clearly erase with **correction fluid** if necessary.
- If a question is wrong, the teacher may decide to nullify it.

Open questions

Answer in the empty space below. Your answer should be carefully justified, and all the steps of your argument should be discussed in details. Leave the check-boxes empty, they are used for the grading.

Question 1: *This question is worth 9 points.*

☐0 ☐1 ☐2 ☐3 ☐4 ☐5 ☐6 ☐7 ☐8 ☐9

Soit G un groupe fini, tel que tous ses éléments non-triviaux sont d'ordre 2.

(a) Montrer que G est abélien.

(b) Soit $H \leq G$ un sous-groupe et $g \in G \setminus H$. Montrer que $H \cup gH$ est un sous-groupe de G.

(c) Montrer que $|H \cup gH| = 2|H|$.

(d) Déduiser qu'il existe un entier $k \geq 0$ tel que $|G| = 2^k$.

Solution:

(a) For any $g \in G$ we have $g^2 = e$ or equivalently $g = g^{-1}$ 1P. Thus any $g, h \in G$ we have

$$gh = (gh)^{-1} \Leftrightarrow gh = h^{-1}g^{-1} \Leftrightarrow gh = hg.1P$$

(b) Clearly $N = H \cup gH$ is non-emtpy, thus it is sufficient to show that N is stable under multiplication and inversion 1P. Stability under inversion follows from the observation that $g^{-1} = g$. For the stability under multiplication we notice that the product of two elements in gH lies in H since $g^2 = e$, and the product of $h \in H$ and $gh' \in gH$ is again in gH 1P.

(c) If is enough to show that H and gH are disjoint 1P, but this is immediate since they're both left cosets 1P.

(d) If $G = \{e\}$ we are done. Otherwise pick $g_1 \in G \setminus \{e\}$ and consider $H_1 = \langle g \rangle$. If $G = H_1$ we're done aswell since $|H_1| = o(g_1) = 2$. If not pick $g_2 \in G \setminus H_1$ and consider $H_2 = H_1 \cup g_2 H_1$. By the previous points H_2 is a subgroup of order 4. Thus if $H_2 = G$ we're done, otherwise we may continue in this manner defining $H_i = H_{i-1} \cup g_i H_{i-1}$ for $g_i \in G \setminus H_{i-1}$. Since G is finite we must have $G = H_k$ for some $k \geq 0$ and $|H_k| = 2^k$. 3P

Question 2: *This question is worth 9 points.*

☐0 ☐1 ☐2 ☐3 ☐4 ☐5 ☐6 ☐7 ☐8 ☐9

(a) Donner la définition du produit semi-directe.

(b) Montrer qu'il existe un unique produit semi-direct non-trivial $\mathbb{Z}/3\mathbb{Z} \rtimes_\phi \mathbb{Z}/4\mathbb{Z}$.

(c) Déterminer l'ordre des éléments $([1], [1])$ et $([1], [2])$ dans $\mathbb{Z}/3\mathbb{Z} \rtimes_\phi \mathbb{Z}/4\mathbb{Z}$.

(d) Montrer que $\mathbb{Z}/3\mathbb{Z} \rtimes_\phi \mathbb{Z}/4\mathbb{Z}$ n'est pas isomorphe à D_{12}

Solution:

(a) For two groups N, H and a homomorphism $\phi : H \to \mathrm{Aut(N)}$ the semi-direct product $N \rtimes_\phi H$ is defined as the set $N \times H$ with the product

$$(n_1, h_1)(n_2, h_2) = (n_1 \phi_{h_1}(n_2), h_1 h_2).1P$$

Here we used the notation $\phi_{h_1} = \phi(h_i) \in \mathrm{Aut(N)}$.

(b) We have seen that $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong (\mathbb{Z}/3\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z}$. 1P Thus the different semi-direct products are given by the homomorphisms $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$. But these are determined by the image of $[1] \in \mathbb{Z}/4\mathbb{Z}$ which has only two possibilities. If $[1]$ gets send to $[0]$ we get the trivial semi-direct product, thus the only non-trivial semi-direct product comes from the homomorphism sending $[1]$ to $[1] \in \mathbb{Z}/2\mathbb{Z}$. 2P Notice that in this case $\phi_{[1]} : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ is multiplication by 2.

(c) We have $([1],[1])^2 = ([0],[2])$, $([1],[1])^3 = ([1],[3])$, $([1],[1])^4 = ([0],[0])$. Thus the order of $([1],[1])$ is 4. 1P
Similarly $([1],[2])^2 = ([2],[0])$, $([1],[2])^3 = ([0],[2])$, $([1],[2])^4 = ([1],[0])$, $([1],[2])^5 = ([2],[2])$, $([1],[2])^6 = ([0],[0])$. Thus the order of $([1],[2])$ is 6. 1P

(d) It follows from Exercise 12.1 that the order of elements in D_{12} always divides 6. In particular D_{12} does not contain any elements of order 4. 3P

Question 3: *This question is worth 9 points.*

☐0 ☐1 ☐2 ☐3 ☐4 ☐5 ☐6 ☐7 ☐8 ☐9

(a) Ecrire les permutations suivantes sous la forme de produits de cycles disjoints:

(i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 7 & 2 & 4 & 1 & 6 \end{pmatrix}$

(ii) $(147)(452)(23)(16)$

(b) Soit $\sigma \in S_6$ la permutation $\sigma = (123456)$. Ecrire tous les éléments dans l'intersection

$$\langle \sigma \rangle \cap A_6,$$

sous la forme de produits de cycles disjoints.

(c) Montrer que pour chaque $\sigma \in S_n$ il existe un $\tau \in S_n$ tel que $\tau\sigma\tau^{-1} = \sigma^{-1}$.

Solution:

(a) (i) $(1376)(254)$ 1P

(ii) (1645237) 1P

(b) Since σ is a cycle of even length we have $sgn(\sigma) = -1$ 1P. Thus $\langle \sigma \rangle \cap A_6 = \{e, \sigma^2, \sigma^4\}$. Now e is the empty cycle, $\sigma^2 = (135)(246)$ and $\sigma^4 = (153)(264)$ 1P.

(c) Let's assume first, that $\sigma = (a_1 a_2 \dots a_r)$ is a cycle. Then for any τ we have the formula

$$\tau\sigma\tau^{-1} = (\tau(a_1)\tau(a_2)\dots\tau(a_r)).1P$$

On the other hand, we have $\sigma^{-1} = (a_r a_{r-1} \dots a_2 a_1)$ 1P. Now if we let τ be the permutation with $\tau(a_i) = a_{r-i+1}$ for $1 \le i \le r$ and $\tau(k) = k$ for $k \notin \{a_1, \dots, a_r\}$, we get $\tau\sigma\tau^{-1} = \sigma^{-1}$. 1P

Now in general we may write $\sigma = \sigma_1 \dots \sigma_k$ as a product of disjoint cycles. For each $1 \le i \le k$ we may pick τ_i as above with $\tau_i\sigma_i\tau_i^{-1} = \sigma_i^{-1}$. Notice that by constuction the supports of the τ_i are pairwise disjoint. Thus if we set $\tau = \tau_1 \cdots \tau_r$. We have

$$\tau\sigma\tau^{-1} = \tau\sigma_1\tau^{-1}\tau\sigma_2\tau^{-1}\cdots\tau\sigma_r\tau^{-1} = \tau_1\sigma_1\tau_1^{-1}\tau_2\sigma_2\tau_2^{-1}\cdots\tau_r\sigma_r\tau_r^{-1} = \sigma_1^{-1}\cdots\sigma_r^{-1} = \sigma^{-1}.2P$$

Question 4: *This question is worth 9 points.*

☐0 ☐1 ☐2 ☐3 ☐4 ☐5 ☐6 ☐7 ☐8 ☐9

(a) Enoncer le Théorème de Lagrange.

(b) Démontrer le Théorème de Lagrange en utilisant les résultats sur les classes à gauche vu dans le cours.

(c) Soit p un nombre premier et G un groupe avec $|G| = p^2$.

(i) Montrer que G contient un sousgroupe H avec $|H| = p$.

(ii) Montrer que G est cyclique si et seulement si G contient un unique sousgroupe H avec $|H| = p$.

Solution

(a) Lagrange's theorem states the following.

Theorem: Let G be a finite group and $H \leq G$ a subgroup. Then $|H|$ divides $|G|$. 1P

(b) To prove the theorem we use two facts about the left cosets of H in G. First, that $\{gH \mid g \in G\}$ forms a partition of G and secondly that $|H| = |gH|$ for all $g \in G$.
Now let $G/H = \{g_1H, \ldots, g_rH\}$ with $r = |G/H|$. Then by the two previous facts we have

$$|G| = \sum_{i=1}^{r} |g_iH| = r|H|. \tag{1}$$

In particular $|H|$ divides $|G|$. 3P

(c) (i) Consider an element $g \in G \setminus \{e\}$. Then $\langle g \rangle \leq G$ is a subgroup different from $\{e\}$ and thus by Lagrange's theorem $|\langle g \rangle| = p$ or p^2. 1P In the first case $\langle g \rangle$ is the desired subgroup. In the second case $G = \langle g \rangle$ is cyclic and $\langle g^p \rangle = \{e, g^p, g^{2p}, \ldots, g^{(p-1)p}\}$ is a subgroup with p elements. 1P

(ii) If G is cyclic, it is isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$. And we have seen in Exercise 7.5 that for a general n proper subgroups of $\mathbb{Z}/n\mathbb{Z}$ are indexed by proper divisors of n. Since the only proper divisor of p^2 is p the statement follows. 1P
For the other direction let H be the unique subgroup and $g \in G \setminus H$. Then $\langle g \rangle$ is a subgroup different from $\{e\}$ and H. By assumption $|\langle g \rangle| \neq p$ and thus by Lagrange's theorem $|\langle g \rangle| = p^2$ which means that $G = \langle g \rangle$ is cyclic. 2P

Question 5: *This question is worth 12 points.*

☐0 ☐1 ☐2 ☐3 ☐4 ☐5 ☐6 ☐7 ☐8 ☐9 ☐10 ☐11 ☐12

(a) Soit $A = \{1, 2, 3, 4, 5, 6, 7\}$. Combien de relations d'équivalence $R \subset A \times A$ existent tel que $(1, 3), (2, 6), (3, 5) \in R$ et $(5, 6) \notin R$? Expliquer votre raisonnement.

(b) Soit A un ensemble fini et $f : A \to A$ une application. On considère l'ensemble $R \subset A \times A$ définie par

$$R = \{(a, b) \in A \times A \mid \exists n \geq 1 : \ b = f^n(a)\}.$$

Ici on utilise la notation $f^n = \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ fois}}$.

(i) Montrer que R est une relation d'équivalence si et seulement si f est une bijection.

(ii) Calculer le cardinal de A/R pour $A = (\mathbb{Z}/10\mathbb{Z})^\times$ et

$$\begin{aligned} f : (\mathbb{Z}/10\mathbb{Z})^\times &\to (\mathbb{Z}/10\mathbb{Z})^\times \\ [a] &\mapsto [a^3]. \end{aligned}$$

Vous pouvez admettre que f est une bijection.

Solution

(a) Any equivalence relation on A determines and is determined by a partition $A = \sqcup A_i$. By the assumptions we may assume $1, 3, 5 \in A_1$, $2, 6 \in A_2$ and $A_1 \neq A_2$ 1P. Then we can put 4 either to A_1, A_2 or into a new subset A_3 1P. In the first two cases, this leaves 3 possibilities for 7, in the last one 4, thus in total $2 \cdot 3 + 4 = 10$. 1P

(b) (i) Let us assume first that R defines an equivalence relation. Then we have in particular for every $a \in A$ that $(a, a) \in R$. This means that there exists an $n \geq 1$ such that $a = f^n(a)$, which in turn implies a lies in the image of f. Since this is true for any $a \in A$ we dedeuce that f is surjective 1P. But A is finite by assumption and thus f must be bijective. 1P
For the other direction lets assume that f is a bijection. We claim that every $a \in A$ there exists an $n \geq 1$ such that $f^n(a) = a$. Indeed, since A is finite the subset,

$$\{f^n(a) \mid n \geq 1\}$$

is also finite and thus there exist $n_1 > n_2$ such that $f^{n_1}(a) = f^{n_2}(a)$. Since f is in particular injective we deduce that $f^{n_1 - n_2}(a) = a$. 2P
This shows reflexivity of R i.e. for every $a \in A$ we have $(a, a) \in R$. For symmetrie let's assume that $(a, b) \in R$ i.e. $b = f^n(a)$ for some $n \geq 1$. Let n' be such that $f^{n'}(a) = a$ and write $n = sn' + r$ with $r < n'$. Then we have

$$b = f^{sn'+r}(a) = f^{(s-1)n'+r}(a) = \cdots = f^r(a).$$

Applying $f^{n'-r}$ on both sides we get $f^{n'-r}(b) = a$ and thus $(b, a) \in R$.2P
Finally for transitivity assume that $(a, b), (b, c) \in R$ i.e. there are $n_1, n_2 \geq 1$ such that $b = f^{n_1}(a)$ and $c = f^{n_2}(b)$. From this we see that $c = f^{n_1+n_2}(a)$ and thus $(a, c) \in R$ 1P.

(ii) First notice that $(\mathbb{Z}/10\mathbb{Z})^\times = \{[1], [3], [7], [9]\}$ 1P. We can then compute that $[1^3] = [1]$, $[3^3] = [7]$, $[7^3] = [3]$ and $[9^3] = [9]$ and from this we see that $|A/R| = 3$ 1P.