# Questions rapides : groupes, anneaux, corps

D. Harari

Agrégation

**1.** Soit $G$ le groupe abélien $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, muni de la loi $+$. Quel est son groupe d'automorphismes ?

R : Un automorphisme de groupes de $G$ est la même chose qu'un automorphisme de $\mathbf{Z}/2\mathbf{Z}$-ev, le groupe d'automorphismes est donc $GL_2(\mathbf{Z}/2\mathbf{Z})$ (qui est non abélien de cardinal 6, donc isomorphe à $\mathcal{S}_3$).

**2.** Le groupe additif $\mathbf{Q}$ est-il engendré par une partie finie ?

**3.** Si $G, H, K$ sont trois groupes avec $K \triangleleft H$ et $H \triangleleft G$, a-t-on toujours $K \triangleleft G$ ?

R : Non. Prendre $G = \mathcal{S}_4$, $H = V_4$ (groupe constitué de l'identité et des doubles transpositions), et pour $K$ le sous-groupe engendré par une transposition.

**4.** Soit $n \in \mathbf{N}^*$, sans facteur carré. Le groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^*$ est-il toujours cyclique ?

Non, par exemple pour $n = 15$, on trouve via le lemme chinois que $(\mathbf{Z}/n\mathbf{Z})^*$ est isomorphe au groupe additif $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$.

**5.** Soit $f : G \to G'$ un morphisme surjectif de groupes. Soit $H'$ un sous-groupe d'indice $e$ de $G'$, quel est l'indice dans $G$ de $f^{-1}(G')$ ?

**6.** Peut-on étendre 5. à un morphisme injectif de groupes ?

**7.** Si un groupe fini a tous ses sous-groupes de Sylow distingués, est-il abélien ?

R : Non, faire le produit d'un 2-groupe non abélien (ex. $H_8$) avec un 3-groupe.

**8.** Si un groupe fini a tous ses Sylow cycliques, est-il toujours abélien ?

R : Non, ex. $\mathcal{S}_3$.

**9.** Montrer que le groupe $\mathcal{S}_4$ est résoluble. Peut-on trouver une suite

$$\{1\} = G_0 \subset G_1 \subset ... \subset G_r = \mathcal{A}_4,$$

où chaque $G_i$ est distingué dans $\mathcal{A}_4$ et les quotients $G_{i+1}/G_i$ sont tous cycliques ?

**10.** Un sous-groupe d'indice 2 d'un groupe fini est-il toujours distingué ? Et d'indice 3 ?

**11.** Quels sont les morphismes de $\mathcal{A}_6$ dans $\mathbf{Z}/2021\mathbf{Z}$ ?

R : Comme le sous-groupe dérivé de $\mathcal{A}_6$ est lui-même et que $\mathbf{Z}/2021\mathbf{Z}$ est abélien, le seul morphisme est le morphisme trivial puisque l'image d'un commutateur de $\mathcal{A}_6$ doit être le neutre.

**12.** Soit $G$ un groupe fini. Montrer que $G$ est abélien si et seulement si toutes ses représentations irréductibles sont de degré 1.

R : Cela résulte facilement de la formule $\sum_{i=1}^{h} n_i^2 = |G|$, où $h$ est le nombre de classes de conjugaison de $G$ et $n_1, ..., n_h$ les degrés de ses représentations irréductibles.

**13.** Soit $K$ un corps. Montrer que le centre de $\mathrm{GL}_n(K)$ (resp. de $\mathrm{SL}_n(K)$) est constitué des matrices scalaires de ce groupe.

**14.** Soit $G$ un groupe fini tel que le quotient de $G$ par son centre soit abélien. Le groupe $G$ est-il toujours abélien ?

R : Non, prendre par exemple le groupe diédral de cardinal 8. Le centre est de cardinal 2, donc le quotient (de cardinal 4) est abélien. Plus généralement, tout $p$-groupe non abélien de cardinal $p^3$ est un contre-exemple, vu que le centre est non trivial et un $p$-groupe de cardinal $\leq p^2$ est abélien.

**15.** Soit $p$ un nombre premier. Quels sont les groupes abéliens finis $(G, +)$ tels que tout élément $x$ de $G$ vérifie $px = 0$ ?

R : Ce sont aussi les $\mathbf{Z}/p\mathbf{Z}$ de dimension finie, donc les $(\mathbf{Z}/p\mathbf{Z})^r$ avec $r$ entier.

**16.** Soit $G$ un groupe admettant une partie génératrice finie. Montrer que $G$ est fini ou dénombrable.

**17.** Soit $K$ un corps. Soit $L$ une extension de $K$. Si $x \in L$ annule un polynôme unitaire à coefficients dans $K$, montrer que $K[x]$ est de dimension finie sur $K$ et que $K[x] = K(x)$.

R : $K[x]$ est de dimension finie sur $K$ car engendré par $(1, x, ...x^{d-1})$, où $d$ est le degré du polynôme minimal de $x$. Ensuite, $K[x]$ est une algèbre intègre de dimension finie sur $K$, donc c'est un corps (si $z \in K[x]$, la multiplication par $z$ est $K$-linéaire et injective de $K[x]$ dans lui-même, donc bijective), donc $K[x] = K(x)$.

**18.** Soit $K$ un corps fini. Soit $L$ une extension finie de $K$. Montrer qu'il existe $\alpha \in L$ tel que $L = K[\alpha]$. En déduire qu'il existe des polynômes irréductibles de tout degré sur $K$.

R : Comme on sait que le groupe multiplicatif $L^*$ est cyclique, on en prend un générateur $\alpha$ et il est alors immédiat que $L = K[\alpha]$ (vu que $L^* = \{1, \alpha, ..., \alpha^{r-1}\}$, où $r$ est l'ordre de $L^*$). Si maintenant $d \in \mathbf{N}^*$, le corps $K$ admet une extension $L$ de degré $d$ sur $K$ (par le théorème d'existence des corps finis). Si $\alpha$ est comme ci-dessus, son polynôme minimal sur $K$ est irréductible de degré $d$.

**19.** Soit $K$ un corps de caractéristique zéro. Montrer que si $P \in K[X]$ est irréductible dans $K[X]$ et si $L$ est une extension de corps de $K$, alors toute racine de $P$ dans $L$ est simple.

**20.** Montrer que le résultat de 19. vaut encore sur un corps parfait de caractéristique $p > 0$ (par exemple un corps fini), mais pas en général.

**21.** Donner un exemple d'anneau factoriel qui n'est pas principal, et d'un anneau intègre qui n'est pas factoriel.

R : L'anneau $\mathbf{Z}[X]$ est factoriel mais pas principal car il ne vérifie pas Bezout (par exemple 2 et $X$ sont premiers entre eux mais il n'y a pas de polynômes $A, B$ de $\mathbf{Z}[X]$ tels que $2A + XB = 1$). On a vu en cours que $\mathbf{Z}[i\sqrt{5}]$ est intègre mais pas factoriel.

**22.** Soit $n$ un entier non nul. Déterminer tous les morphismes d'anneaux de $\mathbf{Z}/4\mathbf{Z}[X]/(X^2)$ dans $\mathbf{Z}/4\mathbf{Z}$.

R : Se donner un tel morphisme revient à se donner un morphisme d'anneaux $\varphi : \mathbf{Z}/4\mathbf{Z}[X] \to \mathbf{Z}/4\mathbf{Z}$ qui s'annule en $X^2$. Un tel morphisme est déterminé par l'image $a$ de $X$, qui doit donc vérifier $a^2 = 0$, soit $a = 0$ ou $a = \bar{2}$. Il y a donc deux morphismes de $\mathbf{Z}/4\mathbf{Z}[X]/(X^2)$ dans $\mathbf{Z}/4\mathbf{Z}$, donnés par $P \mapsto P(a)$ pour ces deux valeurs de $a$.

**23.** Soit $K$ un corps. Soit $F \in K(X_1, ..., X_n)$ une fraction rationnelle symétrique. Peut-on toujours écrire $F$ comme le quotient de deux polynômes symétriques ?

**24.** Montrer que le seul automorphisme de corps de $\mathbf{R}$ est l'identité. Quid des automorphismes du groupe $(\mathbf{R}, +)$ ?

R : Un tel automorphisme induit clairement l'identité sur $\mathbf{Q}$. Il est par ailleurs croissant car l'image d'un carré est un carré, donc l'image d'un réel positif est positif. On voit alors aisément qu'il est continu, donc par densité c'est l'identité. Il y a par contre des automorphismes du groupe $(\mathbf{R}, +)$ (non continus) autre que l'identité : prendre une base de $\mathbf{R}$ en tant que $\mathbf{Q}$-espace vectoriel (existe par Zorn), et définir un automorphisme $\mathbf{Q}$-linéaire de $\mathbf{R}$ en permutant par exemple les vecteurs de cette base.

**25.** L'anneau des fonctions holomorphes de $\mathbf{C}$ dans $\mathbf{C}$ est-il intègre ? Est-il principal ?

**26.** Soit $A$ un anneau intègre fini. Montrer que $A$ est un corps. Et si $A$ est une $K$-algèbre intègre de dimension finie sur $K$, où $K$ est un corps ?

**27.** Un anneau commutatif est dit local si l'ensemble de ses éléments non inversibles est un idéal. Donner un exemple d'anneau local intègre qui n'est pas un corps. Existe-t-il des anneaux locaux non intègres ?

R : On peut prendre $A = \mathbf{C}[[T]]$, l'ensemble des non inversibles est l'idéal engendré par $T$. PAr ailleurs $\mathbf{Z}/4\mathbf{Z}$ est local non intègre.

**28.** Montrer que tout sous-groupe de $\mathbf{Z}^n$ est isomorphe à $\mathbf{Z}^r$ avec $r \leq n$.

**29.** Les corps $\mathbf{C}$ et $\mathbf{C}(T)$ sont-ils isomorphes ?

**30.** Montrer que dans un anneau principal, tout idéal premier non nul est maximal. Cette propriété caractérise-t-elle les anneaux principaux parmi les anneaux intègres ?