

Planche 1.

Question de cours. Est ce que tout anneau est un corps ?

Exercice 1. Soit G un groupe et H, K deux sous-groupes. Montrer que $H \cap K$ est un sous-groupe de G .

Exercice 2. Montrer que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement n est premier.

Exercice 3. On dit que $G = (S, A)$ est un graphe si S est un ensemble (les sommets), A est une partie de $S \times S$ (les arêtes) tel que si $(x, y) \in A$ alors $(y, x) \in A$.

Un automorphisme f de G est une bijection de S dans S tels que $(f(s), f(s')) \in A \iff (s, s') \in A$.

Soit G un graphe, montrer que l'ensemble des automorphismes forme un groupe pour la loi de composition.

Planche 2.

Question de cours. Est ce que tout anneau est intègre ?

Exercice 1. Soit G un groupe. On pose $Z(G) = \{a \in G : ax = xa, \forall x \in G\}$. Montrer que $Z(G)$ est un sous-groupe de G .

Exercice 2. Trouver les sous-groupes de $(\mathbb{Z}/p\mathbb{Z}, +)$ où p est un nombre premier.

Exercice 3. Montrer que $(\mathbb{Z}, +)$ et $(\mathbb{Z}^2, +)$ ne sont pas isomorphes.

Planche 3.

Question de cours. Soit $(A, +, \times)$ un anneau. Est ce que (A, \times) est un groupe ?

Exercice 1. Soit G un groupe et H un sous-groupe de G . Soit $a \in G$, montrer que $aHa^{-1} = \{aha^{-1}, h \in H\}$ est un sous-groupe de G .

Exercice 2. Soit G un groupe, H et K deux sous groupes de G . On pose $HK = \{hk, h \in H, k \in K\}$. Trouver une condition nécessaire et suffisante sur H et K pour que HK soit un sous-groupe de G .

Exercice 3. Trouver les nilpotents de $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

Solutions - Planche 1.

Question de cours. Non, par exemple $(\mathbb{Z}, +, \times)$ est un anneau et 2 n'est pas inversible pour x . En effet, si 2 l'était alors il existerait un entier a tel que $2a = 1$, mais ce n'est pas possible d'après la décomposition en facteurs premiers.

Exercice 1. Le neutre étant dans H et K , il est bien dans $H \cap K$. Soit $g, h \in H \cap K$. Alors $g \in H$ et $h \in H$. Donc $gh \in H$. De même $gh \in K$ donc $gh \in H \cap K$.

De plus $g^{-1} \in H$ car $g \in H$ et $g^{-1} \in K$ car $g \in K$. D'où $g^{-1} \in H \cap K$.

Finalement $H \cap K$ est non vide, est stable pour la loi de G et est stable par inversion.

Donc $H \cap K$ est un sous-groupe de G .

Exercice 2. $\mathbb{Z}/n\mathbb{Z}$ est un anneau pour tout n .

→ Supposons que n soit premier. Soit $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ avec $a \in \mathbb{Z}$ et $\bar{a} \neq 0$. On cherche à montrer que a est inversible. Pour cela il faut utiliser le fait que n est premier. Traduisons $\bar{a} \neq 0$ en arithmétique : cela veut dire que n ne divise pas a . Donc a est premier à n (car n est un nombre premier). Donc [réflexe], le théorème de Bézout dit qu'il existe u et v deux entiers tels que $au + vn = 1$.

Passons au modulo : on obtient $\bar{a}\bar{u} + \bar{v}\bar{n} = \bar{1}$. Or $\bar{n} = \bar{0}$ donc \bar{a} admet un inverse. Donc $\mathbb{Z}/n\mathbb{Z}$ est un corps.

→ Supposons que $\mathbb{Z}/n\mathbb{Z}$ soit un corps. Montrons que n soit premier. Si ce n'était pas le cas, alors il existerait u et v deux entiers naturels différents de 1 et n tels que $n = uv$. Donc $\bar{u}\bar{v} = \bar{0}$ avec $\bar{u} \neq 0$ et $\bar{v} = 0$. Cela contredit le fait que $\mathbb{Z}/n\mathbb{Z}$ soit intègre (car c'est un corps). Donc n est premier.

Exercice 3. L'identité de S est bien un automorphisme de G . En effet il s'agit d'une bijection de S dans S et de plus on a bien $\forall s, s' \in S, (f(s), f(s')) \in A \iff (s, s') \in A$ pour $f = id$.

Soit f et g deux automorphismes de G . Montrons que la composée est encore un automorphisme de G . D'après le cours, la composée de deux bijections est encore une bijection, il reste à vérifier que $f \circ g$ conserve bien les arêtes. Soit s, s' deux sommets. Alors comme f est un automorphisme de G :

$$(f(g(s)), f(g(s'))) \in A \iff (g(s), g(s')) \in A$$

Or comme g est un automorphisme de G , alors $(g(s), g(s')) \in A \iff (s, s') \in A$. Donc $f \circ g$ est bien un automorphisme de G .

Soit f un automorphisme de G . f^{-1} est encore une bijection de S . Soit s, s' deux sommets. Alors, comme f est un automorphisme de G :

$$(f^{-1}(s), f^{-1}(s')) \in A \iff (f(f^{-1}(s)), f(f^{-1}(s'))) \in A \iff (s, s') \in A$$

D'où f^{-1} est encore un automorphisme de G . Donc il s'agit bien d'un sous-groupe des automorphismes de S .

Questions en plus : Trouver un graphe G tel que $Aut(G) = S_n$. Réponse : K_n la clique : n sommets tous reliés entre eux.

[*] Trouver un graphe non trivial G tel que $Aut(G) = id$.

[*] Montrer qu'un automorphisme de G conserve les degrés. Sachant que le degré d'un sommet est le nombre de voisins (de sommets reliés à ce sommet) qu'il a. Preuve : soit f un automorphisme de G . Soit v un sommet. On note $d = \deg(v)$ le degré de v . Alors il existe v_1, \dots, v_d des sommets distincts tels que v_i soit relié à v pour tout i . Alors $f(v_i)$ est relié à $f(v)$ pour tout i . Donc $f(v)$ a au moins d voisins. Soit s un autre sommet tel que s est relié à $f(v)$. On pose s' tel que $f(s') = s$. Alors comme $f(s')$ est relié à $f(v)$ alors s' est relié à v donc $s' = s_i$ pour un certain i . Donc $s = f(v_i)$. Donc $f(v)$ n'admet pas d'autres voisins. Donc $\deg(f(v)) = \deg(v)$.

[**] Soit G_1, \dots, G_c les composantes connexes de G . Alors $Aut(G) = Aut(G_1) \times \dots \times Aut(G_c)$. Cela montre en disant qu'un sommet v est envoyé sur un autre sommet de la composante connexe (car sinon il existerait un chemin entre deux composantes connexes). Donc chaque composante connexe est stable par les automorphismes.

Solutions - Planche 2.

Question de cours. Non, $\mathbb{Z}/4\mathbb{Z}$ n'est pas intègre. En effet on a $\bar{2}\bar{2} = \bar{0}$.

Exercice 1. L'élément neutre de G est dans $Z(G)$ (car il commute avec tout le monde). Soit $a, b \in Z(G)$. Soit $g \in G$. $abg = a(bg) = a(gb) = (ag)b = (ga)b = gab$. Donc ab commute avec G . Donc $ab \in Z(G)$.

Soit $a \in Z(G)$. Soit $g \in G$. Alors $a^{-1}g = a^{-1}gaa^{-1} = a^{-1}aga^{-1} = ga^{-1}$ car a commute avec G . Donc $a^{-1} \in Z(G)$.

Donc $Z(G)$ est un sous-groupe de G .

Exercice 2. Soit H un sous-groupe de $\mathbb{Z}/p\mathbb{Z}$ différent de $\{\bar{0}\}$. On note $\bar{a} \in H$ l'élément de H tel que $\bar{a} \neq \bar{0}$ et a soit le plus petit des représentants positifs. Donc $a < p$. Donc a est premier à p . Donc [réflexe] d'après le théorème de Bézout, il existe u, v deux entiers tels que $au + vp = 1$. Donc $\bar{a}\bar{u} = \bar{1}$. Donc $\bar{u} = \bar{a}^{-1} \in H$. Donc $\bar{1} \in H$. Donc $H = \mathbb{Z}/p\mathbb{Z}$.

Les sous-groupes de $\mathbb{Z}/p\mathbb{Z}$ sont donc triviaux (il n'y a que le sous-groupe constitué uniquement du neutre et le groupe entier lui-même).

Exercice 3. On raisonne par l'absurde. Supposons qu'il existe f un isomorphisme entre $(\mathbb{Z}, +)$ et $(\mathbb{Z}^2, +)$.

On pose $(a, b) = f(1)$. Comme f est surjective, il existe $\lambda \in \mathbb{Z}$ tel que $f(\lambda) = (1, 0)$. Or comme f est un morphisme, $f(\lambda) = \lambda f(1) = (\lambda a, \lambda b)$. Donc $\lambda b = 0$. Or $\lambda \neq 0$ car $f(0) = (0, 0)$. Donc $b = 0$.

De la même manière, en utilisant $(0, 1)$ on montre que $a = 0$. Ce qui contredit l'injectivité de f car $f(0) = f(1) = (0, 0)$.

Ces deux groupes ne sont donc pas isomorphes.

Solutions - Planche 3.

Question de cours. Non, (\mathbb{Z}, \times) n'est pas un groupe. \times est bien une loi de composition interne associative et admet 1 pour neutre. Mais tout élément n'est pas inversible. En effet 2 n'est pas inversible. Sinon il existerait un entier a tel que $2a = 1$, mais ce n'est pas possible d'après la décomposition en facteurs premiers.

Exercice 1. Soit y et z deux éléments de aHa^{-1} . Alors il existe h et h' de H tels que : $y = aha^{-1}$ et $z = ah'a^{-1}$. Donc :

$$yz = aha^{-1}ah'a^{-1} = ah'h'a^{-1} \in aHa^{-1}$$

Donc le produit est stable. De plus le neutre e est bien dans aHa^{-1} car $e = aea^{-1} = aa^{-1}$. De plus :

$$y^{-1} = (aha^{-1})^{-1} = (a^{-1})^{-1}h^{-1}a^{-1} = ah^{-1}a^{-1}$$

Donc c'est aussi stable par inversion. Donc aHa^{-1} est un sous-groupe de G .

Exercice 2. Méthode : pour trouver la CNS on suppose que HK est un sous-groupe de G . On utilise les propriétés que doit vérifier le sous-groupe pour obtenir des propriétés que doit vérifier le groupe G .

→ Supposons donc que HK soit un sous-groupe de G . Alors HK contient l'élément neutre e . Donc $e = hk$ pour un $h \in H$ et $k \in K$. Mais cela ne donne rien car l'égalité $e = ee$ est toujours vraie dans G .

HK est stable par produit. Soit $h, h' \in H$ et $k, k' \in K$, alors $hkh'k' \in HK$ par hypothèse sur HK . Donc il existe $h'' \in H$ et $k'' \in K$ tels que $hkh'k' = h''k''$. Donc $kh' = h^{-1}h''k''k'^{-1} \in HK$. Ca par contre c'est pas normal parce que H et K commutent pas forcément. Comme l'égalité précédente est vraie pour tout $k \in K$ et $h' \in H$, alors $KH \subset HK$. Du coup la CNS à montrer comporte déjà $KH \subset HK$. De plus $(hk)^{-1} = k^{-1}h^{-1}$ n'apporte rien de plus donc la CNS est $KH \subset HK$.

→ Supposons que $HK = KH$. Alors e est bien dans HK . Soit $h, h' \in H$ et $k, k' \in K$. Alors il existe $h'' \in H$ et $k'' \in K$ tels que :

$$hkh'k' = h(kh')k' = h(h''k'')k' = hh''k''k' \in HK$$

Donc HK est bien stable par produit car $KH \subset HK$.

De plus $(hk)^{-1} = k^{-1}h^{-1}$. Donc il existe h'' et k'' tels que $(hk)^{-1} = h''k'' \in HK$. Donc l'inverse est bien dans HK . Donc HK est bien un sous-groupe de G .

Ainsi HK est un sous-groupe de G ssi $KH \subset HK$.

Exercice 3. Soit x un nilpotent de $\mathbb{Z}/n\mathbb{Z}$. Alors il existe un entier positif k tel que $x^k = 0$. Donc $n|x^k$. Cela va donner des informations quant aux nombres premiers contenus dans x .

D'après le théorème de décomposition des entiers en premiers, il existe p_1, \dots, p_s des premiers et des entiers a_i tels que :

$$n = \prod_{i=1}^s p_i^{a_i}$$

Donc n divise x^k cela dit que p_i divise x pour tout i . On pourrait dire plus mais cela va suffire à caractériser les nilpotents.

En effet soit x un entier tel que p_i divise x pour tout i . Alors on pose $k = \max a_i$. Donc $p_i^{a_i}$ divise x pour tout i car $k \geq a_i$. Donc n divise x^k .

On appelle $r = \prod_{i=1}^s p_i = \text{rad}(n)$ de n . Alors x est nilpotent ssi $\text{rad}(n)$ divise x .