# Programme de colle Groupes Anneaux Corps

Classe de MP$^\star$

Lycée du Parc

**Exercice 1 (ddl)**
Soit $(G,.)$ un groupe de cardinal $2n$.
a) Justifier que l'on définit une relation d'équivalence $\mathcal{R}$ sur $G$ en posant

$$x\mathcal{R}y \Leftrightarrow x = y \text{ ou } x = y^{-1}$$

b) En déduire l'existence dans $G$ d'un élément d'ordre 2.

**Indication :** a) L'écrire.
b) Décrire les orbites, regarder celle de l'identité, compter. □

**Exercice 2 (ddl, X)**
Soit $G$ un groupe multiplicatif de cardinal $p^\alpha$ avec $p$ premier et $\alpha \in \mathbb{N}^\star$.
Montrer que

$$Z(G) \neq \{1\}$$

**Indication :** Action : $x \mapsto gxg^{-1}$. Burnside. □

**Exercice 3 (ddl)**
Un sous-groupe d'un groupe produit est-il nécessairement produit de deux sous-groupes ?

**Indication :** Regarder $\mathbb{Z} \times \mathbb{Z}$, géométrique. □

**Exercice 4**
Soient $H$ et $K$ des sous-groupes d'un groupe $G$. On note $HK = \{h.k \mid h \in H \text{ et } k \in K\}$.

**1)** Lorsque $G$ est fini, déterminer le cardinal de $HK$.

**2)** Montrer que $HK$ est un sous-groupe de $G$ si et seulement si $HK = KH$.

**Solution.**

**1)** Soit $f : H \times K \to HK$ définie par $f(h,k) = hk$. On montre que $f^{-1}(hk) = \{(hu^{-1}, uk) \mid u \in H \cap K\}$.

**2)** Sens direct : Soit $h.k \in HK$, qui est un sous-groupe, donc il existe $h' \in H$ et $k' \in K$ tels que $hkh'k' = 1$. En multipliant par $k'^{-1}h'^{-1}$ à droite, on trouve $hk = k'^{-1}h'^{-1} \in KH$. Donc $HK \subset KH$. Par une démarche analogue (mais non symétrique !), on a l'inclusion réciproque.
Réciproquement, si $h_1.k_1$ et $h_2.k_2 \in HK$, il existe $h \in H$ et $k \in K$ tels que $hk = k_1.k_2^{-1}h_2^{-1}$. Alors $h_1k_1.k_2^{-1}h_2^{-1} = (h_1h)k \in HK$.

□

**Exercice 5 (ddl)**
Un sous-groupe $H$ de $(G,.)$ est dit distingué si

$$\forall x \in H, \forall a \in G, axa^{-1} \in H$$

**1)** Montrer que le noyau d'un morphisme de groupes au départ de $(G,.)$ est distingué.

**2)** Montrer que $G/H$ muni de la loi induite est un groupe lorsque $H$ est distingué. En déduire que tout sous-groupe distingué est le noyau d'un morphisme de groupe.

**3)** Soient $H, K$ deux sous-groupes de $(G, .)$.
On suppose le sous-groupe $H$ distingué, montrer que l'ensemble

$$HK = \{xy / x \in H, y \in K\}$$

est un sous-groupe de $(G, .)$.

**4)** Notons $p : G \to G/H$ la projection et $K$ un sous-groupe de $G$ tel que $p(K) = G/H$ et $|K| = |G/H|$. Montrer que $H \cap K = \{1\}$ puis que $G = HK$.

**5)** On note $D(G) =< \{xyx^{-1}y^{-1} \mid (x, y) \in G^2\} >$. Montrer que c'est un sous-groupe distingué.

**6)** Montrer que $D(G)$ est le plus petit sous-groupe qui « rend » $G$ abélien : pour tout $u : G \to A$, avec $A$ un groupe abélien, montrer qu'il existe $\bar{u}$ telle que $u : G \xrightarrow{p} G/D(G) \xrightarrow{\bar{u}} A$.

**Indication :** 4) produit semi-direct. Par l'absurde ($h \in H \cap K$ vérifie $p(h) = \bar{1}$, s'il y en a 2 problème de cardinal, car $p_{|K}$ bijective). Regarder le noyau de $\varphi : H \times K \to G$. □

**Exercice 6 (ddl, X)**
a) Montrer que tout sous-groupe additif de $\mathbb{R}$ qui n'est pas monogène est dense dans $\mathbb{R}$.
b) Soit $x \in \mathbb{R} \backslash \mathbb{Q}$. Montrer qu'il existe une infinité de $(p, q) \in \mathbb{Z} \times \mathbb{N}^\star$ tels que

$$\left| x - \frac{p}{q} \right| < \frac{1}{q^2}$$

c) Montrer la divergence de la suite de terme général

$$u_n = \frac{1}{n \sin n}$$

**Indication :** a) Montrer que $0 \in \overline{H}$, puis ramener en 0 n'importe quel $x$ par le groupe.
b) Tiroirs pour $f : \{0, N\} \to [0, 1[$ définie par $f(k) = kx - E(kx)$.
c) Appliquer à $\pi$, montrer qu'une suite extraite est plus grande que $\frac{1}{\pi}$. Montrer que $\{\sin(n)\}$ est dense dans $[-1, 1]$ (conséquence de a)) puis qu'une suite extraite converge vers 0 □

**Exercice 7 (ddl)**
Soit $H$ un sous-groupe strict d'un groupe $(G, \star)$. Déterminer le groupe engendré par le complémentaire de $H$ dans $G$.

**Indication :** Montrer que $\langle K \rangle = G$. (Il manque seulement $H$). □

**Exercice 8**
Soit $E$ un ensemble fini, muni d'une loi de composition interne $\star$ associative. Tous les éléments sont réguliers à gauche ($xa = xb \Rightarrow a = b$) et à droite ($ax = bx \Rightarrow a = b$).

**1)** Soit $a \in E$. Notons $s_a : E \to E$ définie par $s_a(x) = a \star x$. Montrer que $s_a$ est bijective.

**2)** Montrer que $\forall (a, x) \in E^2\ \exists p_0 \in \mathbb{N}^*\ a^{p_0} x = x$.

**3)** Montrer qu'il existe $p$ tel que $a^p$ soit un éléments neutre à gauche de $E$.

**4)** Montrer que $a^p$ est l'élément neutre de $E$.

**5)** Montrer que $(E, \star)$ est un groupe.

**Solution.** □

**Exercice 9 (Connexité dans** Spec$A$**)**
Soit $A$ un anneau unitaire commutatif. Montrer que $A$ contient des idempotents différents de 0 et de 1 si et seulement si $A$ est isomorphe à $B \times C$ où $B$ et $C$ sont deux anneaux non nuls.

**Solution.** Réciproque : $e = (1, 0)$. Sens direct : $A \to eA \times (1 - e)A$, en prouvant que ce sont des anneaux. □

**Exercice 10**
Un anneau commutatif $A$ est dit factoriel s'il existe un ensemble $\mathscr{P}$ d'éléments irréductibles de $A$ tels que tout élément de $x \in A$ se décompose de façon unique (à un inversible près et à permutation près) en un produit d'éléments de $\mathscr{P}$ :

$$x = u \prod_{p \in \mathscr{P}} p^{v_p(x)}$$

1) Montrer que $\mathbb{Z}[X]$ est factoriel. On pourra utiliser $c(P) = pgcd(a_i)$ où les $a_i$ sont les coefficients de $P$ pour montrer que $\mathscr{P} = \{p \in \mathbb{Z} \mid p \text{ premier}\} \cup \{P \in \mathbb{Z}[X] \mid P \text{ unitaire et premier dans } \mathbb{Q}[X]\}$.
2) Montrer que si $A$ est factoriel, alors $A[X]$ est factoriel.
3) En déduire que $K[X_1, \ldots, X_n]$ est factoriel.

**Indication :** 1) On admettra que $\mathbb{Z}$ et $K[X]$ sont factoriel (cours). 3) $K[X, Y] = K[X][Y]$. □

**Exercice 11**
1) Montrer que $\mathbb{Z}[i\sqrt{2}]$ est principal.
2) Montrer que $y^3 = x^2 + 2$ a pour unique solutions $(\pm 5, 3)$.

**Indication :**
1) Soit $I$ un idéal non nul, et $a \in I - \{0\}$ de module minimal.
Écrire $b \in I$ sous la forme $b = az + ar$ où $z \in \mathbb{Z}[i\sqrt{2}]$ et $|r| < 1$. Par minimalité de $|a|$ dans $I$, $r = 0$.
2) $y^3 = x^2 + 2 = (x + i\sqrt{2})(x - i\sqrt{2})$. Ces deux derniers nombres sont premiers entre eux dans $\mathbb{Z}[i\sqrt{2}]$. Ils divisent un cube donc ce sont chacun des cubes : $(x + i\sqrt{2}) = (a + ib\sqrt{2})^3$. En développant et en étudiant les valeurs possibles de $a$ et $b$, on trouve $(x, y) = (\pm 5, 3)$.

□