A

1. $\sigma = (1\,6\,9\,2\,3)(4\,7\,8)$; $\tau = (136)(235)(146) \underset{\uparrow}{=} (14)(2635)$

décomposition en cycles disjoints

$\Rightarrow |\tau| = 2 \vee 4 = 4$

2. $(A,+)$ est un gp de cardinal 36, $(B,+)$ est un gp de cardinal 42

On a (d'après le cours)

$$\begin{cases} G \text{, groupe de cardinal } N\text{, est cyclique} \iff G \simeq \mathbb{Z}/N\mathbb{Z} \\ \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/nm\mathbb{Z} \iff n \wedge m = 1 \end{cases}$$

donc $(A,+)$ n'est pas cyclique, $(B,+)$ est cyclique

car (A) = ordre de $(\bar{1},\bar{1})$ dans $(A,+)$ $= 3 \vee 12 = 12$

car (B) = ordre de $(\bar{1},\bar{1})$ dans $(B,+)$ $= 3 \vee 14 = 42$

B

1. Soit K un corps. Alors $\dfrac{K[x]}{(p(x))}$ corps $\iff$ $p(x)$ irréductible dans $K[x]$

d'après un résultat du cours

x^2+x+2 est irred sur $\mathbb{F}_2$ (car de degré 2 et sans racines)

$(x-2)^2(x^2-4x+2)$ est réductible sur $\mathbb{Q}$

$\Rightarrow$ A est un corps, B ne l'est pas.

2. $(x^2+x+2) = (2x+1)^2+1$ (on oubliera de souligner la classe d'un élément dans $\mathbb{F}_3$)

donc dans A

$[2x+1]^2 = [-1] = [2]$ (où $[-]$ dénote la classe d'un élément dans le produit)

$\Rightarrow$ l'inverse de $[\bar{2}x+1]$ est $[\bar{2}]^{-1}[2x+1] = [x+2]$

3. la classe de $\alpha(x-2)$ $(\forall \alpha \in \mathbb{Q}\setminus\{0\})$ [ou celle de $\alpha(x-2)^2$, ou celle de $\alpha(x-2)(x^2-4x+2)$] est un diviseur de zéro dans B.

(4.) les éléments nilpotents sont les classes de

$$\alpha(x-2)(x^2-4x+2) \qquad \forall \alpha \in \mathbb{Q}\setminus\{0\}$$

(5.) $G = \{ [1], [2], [x], [2x], [x+1], [x+2], [2x+1], [2x+2] \}$

les ordres sont respectivement $-, 2, 8, 8, 8, 4, 4, 8$

(6.) L'ordre de $[x]$ est 8 donc le gp engendré par $[x]$ a 8 éléments puisque G aussi est un gp à 8 éléments on a $G = \langle [x] \rangle$ donc G est cyclique

(7.) G est un gp cyclique de cardinal 8 $\Rightarrow$ pour tout diviseur de 8, il existe un unique sousgps de cardinal ce diviseur
On a donc 4 sousgps dans G

$G = \langle [x] \rangle = \langle [2x] \rangle = \langle [x+1] \rangle = \langle [2x+2] \rangle$ (card $= 8$)

$\{1\} = \langle [1] \rangle$ (card $= 1$)

$\langle [2] \rangle$ (card $= 2$)

$\langle [x+2] \rangle = \langle [2x+1] \rangle$ (card $= 4$)

[C]

(1.) $\mathcal{R}$ est une relation d'équivalence sur l'ensemble X. X est donc la réunion disjointe de ses classes $\Rightarrow$

n° classes $= N/r$

(2.) Soit G un gp fini et $H \leq G$, on définit 2 rel. d'ép. sur G

$x \mathcal{R}^g_H y \iff x^{-1}y \in H$, $\qquad x \mathcal{R}^d_H y \iff xy^{-1} \in H$

Les classes pour $\mathcal{R}^g_H$ sont les xH $(x \in G)$
" " $\mathcal{R}^d_H$ " " Hx "

les classes ont toutes le même cardinal, égal à $|H|$, puisque on a des bijections :

$$H \longrightarrow Hx \qquad\qquad H \longrightarrow xH$$
$$h \longmapsto hx \qquad\qquad h \longmapsto xh$$

On applique donc 1 pour obtenir :

n^o classes à droite $=$ n^o classes à gauche $= |G|/|H|$

$\boxed{D}$

1.) A anneau comm. intègre. A est dit factoriel si $a \in A \setminus (A^* \cup \{0\}) \Rightarrow \exists\, p_1, \ldots, p_r$ irreductibles et $a = p_1 \cdots p_r$. En plus si $p_1 \cdots p_r = q_1 \cdots q_s$ ($\exists\, p_i, q_j$ irreductibles) alors $r = s$ et il existe une bijection $\sigma \in S_r$ t.q. $p_i \sim q_{\sigma(i)}$ (où $\sim$ signifie 'associé')

$\mathbb{Z}$ est un anneau factoriel, $\mathbb{Z}[i\sqrt{5}]$ n'est pas un anneau factoriel

2.) $a, b \in A \setminus (\{0\} \cup A^*)$ A factoriel $\Rightarrow$ $\exists\, p_1, \ldots, p_r$ irred. et $\alpha_i, \beta_i \in \mathbb{N}$ t.q. $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ $b = p_1^{\beta_1} \cdots p_r^{\beta_r}$

Alors le pgcd de a et b est $d = p_1^{\min\{\alpha_1, \beta_1\}} \cdots p_r^{\min\{\alpha_r, \beta_r\}}$

" ppcm " " $m = p_1^{\max\{\alpha_1, \beta_1\}} \cdots p_r^{\max\{\alpha_r, \beta_r\}}$

3.) $a, b, c \in A \setminus (\{0\} \cup A^*)$ $a \mid bc \Rightarrow \exists\, d \in A$ et $ad = bc$. On ecrit a, b, c, d comme produit d'irreductibles

$$a_1 \cdots a_r\, d_1 \cdots d_s = b_1 \cdots b_n \cdot c_1 \cdots c_m$$

l'unicité de l'ecriture comme produit d'irreductible implique que chaque a_i $(i = 1, \ldots, r)$ est associé à un b_j ou à un c_k

mais $a \wedge b = 1$ $\Rightarrow$ la première hypothèse est à exclure.

Donc $\forall i=1,\dots,r \quad \exists j\in\{1,\dots,m\}$ et $a_i \sim c_j$

$\Rightarrow a | c$.

E

(1.) Supposons par l'absurde qu'il existe $g\in G$ tq. $|g|=\infty$

On a donc que, $\forall n\in\mathbb{N}$, $\langle g^n\rangle$ est un sous gp de G

et

$$\bigcap_{\{1\}\neq H\leq G} H \subseteq \bigcap_{n\in\mathbb{N}\setminus\{0\}} \langle g^n\rangle \underset{(*)}{=} \{1\}$$

explication de $(*)$

Soit $x\in \bigcap_{n\in\mathbb{N}\setminus\{0\}} \langle g^n\rangle$ Alors $x\in\langle g\rangle \Rightarrow \exists n_1$ et

$x=g^{n_1}$. Mais aussi $\forall i\geq 2 \quad x\in\langle g^i\rangle$, donc il existe $n_i\in\mathbb{Z}$ et $x=g^{i\cdot n_i}$

$|g|=\infty \Rightarrow (g^r=g^s \Leftrightarrow r=s)$

On a donc

$$n_1 = 2n_2 = 3n_3 = 4n_4 = 5n_5 = \dots = i n_i$$

$\forall i\geq 2$

$\Rightarrow n_1$ est divisible par tout entier positif

ABSURDE

$\square$

(2) $\dfrac{\mathbb{Q}[x]}{(x^2-2)}$ est un corps car x^2-2 est irred. sur $\mathbb{Q}$

L'application $\begin{array}{rcl}\mathbb{Q}[x] & \longrightarrow & \mathbb{Q}[\sqrt{2}] \\ p(x) & \longmapsto & p(\sqrt{2})\end{array}$ est un morphisme surjectif d'anneaux de noyau l'idéal (x^2-2)

Donc le thm. d'isomorphisme nous donne

$$\frac{\mathbb{Q}[x]}{(x^2-2)} \simeq \mathbb{Q}[\sqrt{2}]$$

En particulier $\mathbb{Q}[\sqrt{2}]$ est un corps. On sait que $\mathrm{Frac}(\mathbb{Z}[\sqrt{2}])$ est le plus petit corps qui contient $\mathbb{Z}[\sqrt{2}]$. Soit donc K un corps t.q. $K \supseteq \mathbb{Z}[\sqrt{2}]$. Il nous faut demontrer que $K \supseteq \mathbb{Q}[\sqrt{2}]$

$$\mathbb{Z}[\sqrt{2}] \subseteq K \quad \Rightarrow \quad \mathbb{Z} \subseteq K, \ \sqrt{2} \in K$$

$$\left(\begin{array}{l} K \text{ corps} \\ \mathbb{Z}[\sqrt{2}] \subseteq K \end{array}\right. \quad \Rightarrow \quad a/b + c/d\sqrt{2} \in K \quad \forall\, a,b,c,d \in \mathbb{Z},\ b,d \neq 0$$

et donc $\mathbb{Q}[\sqrt{2}] \subseteq K$ $\square$