Exo 1

a) Soit A un anneau principal et soient $a, b \in A$.
Soit d t.q. $(a,b) = (d)$ Alors d est le pgcd de a et b. En particulier si $d = a \wedge b$ alors il existent $\alpha, \beta \in A$ et $d = \alpha a + \beta b$

demo Il faut d.p. $\begin{cases} d|a \quad d|b \\ \text{si } d'|a, d'|b \text{ alors } d'|d \end{cases}$

Or
$a \in (d) \Rightarrow d|a$, $b \in (d) \Rightarrow d|b$.

Ensuite
si $d'|a, d'|b$ on a $a = d'a'$, $b = d'b'$. Puisque $d \in (a,b)$ on a $d = \alpha a + \beta b = d'(\alpha a' + \beta b')$ et donc $d'|d$ □.

b) $I = (f,g) = (d)$ si d = pgcd de f et g
$J = (f) \cap (g) = (m)$ si m = ppcm de f et g

Or $f = (x+\bar{3})(x+\bar{2})$ $g = (x+\bar{3})(x^3+x+\bar{1})$ et

$x^3+x+\bar{1}$ est irred. sur $\mathbb{Z}/5\mathbb{Z}$ (car sans racines et de degré 3)

Donc $f \vee g = (x+\bar{3})(x+\bar{2})(x^3+x+\bar{1})$
$f \wedge g = x+\bar{3}$

Soit $A = \dfrac{\mathbb{Z}/5\mathbb{Z}[x]}{(x+\bar{3}) = I}$ $B = \dfrac{\mathbb{Z}/5\mathbb{Z}[x]}{((x+\bar{3})(x+\bar{2})(x^3+x+\bar{1})) = J}$

Le théorème de correspondance donne

Idéaux de A : A, $\{0_A\}$

Idéaux de B : $(x+\bar{3})/J$, $(x+\bar{2})/J$, $(x^3+x+\bar{1})/J$,

$((x+\bar{3})(x+\bar{2}))/J$, $((x+\bar{3})(x^3+x+\bar{1}))/J$,

$((x+\bar{2})(x^3+x+\bar{1}))/J$, $\{0_B\}$, B.

Exo 2

a) A est un corps $\Leftrightarrow$ $(x^2+\bar{5})$ est un idéal maximal

$\Leftrightarrow$ $(x^2+\bar{5})$ est un idéal premier

car dans un anneau principal un idéal est premier si et seulement si il est maximal.

$(x^2+\bar{5})$ est premier $\Leftrightarrow$ $x^2+\bar{5}$ est un élément premier

$\Leftrightarrow$ $x^2+\bar{5}$ est un irréductible

car dans un anneau factoriel un élément est premier si et seulement si il est irréductible

Or $x^2+\bar{5}$ a degré 2 donc il est irréd. $\Leftrightarrow$ il n'a pas de racines.

$x^2+\bar{5}$ a une racine $\Leftrightarrow$ $-\bar{5}$ est un carré de $\mathbb{Z}/7\mathbb{Z}$

Carrés de $\mathbb{Z}/7\mathbb{Z}$:

$\mathbb{Z}/7\mathbb{Z} \ni \bar{a}$	$\bar{a}^2$
$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$
$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{2}$
$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{4}$
$\bar{6}$	$\bar{1}$

Donc $x^2+\bar{b}$ est réductible $\Leftrightarrow -\bar{b} = \bar{1}, \bar{2}, \bar{4}$

$\Leftrightarrow \bar{b} = \bar{6}, \bar{5}, \bar{3}$

Donc A est un corps $\Leftrightarrow \bar{b} = \bar{1}, \bar{2}, \bar{4}$

b) $\bar{b}=\bar{4} \Rightarrow A$ est un corps $\Rightarrow (A\setminus\{0_A\}, \cdot)$ est un gp.

On cherche le plus petit entier positif n t.q. $[x]^n = [1]$

Or $[x]^2 = [-4] = [\bar{3}]$ et $\bar{3}$ est un élément d'ordre

6 dans $(\mathbb{Z}/72\mathbb{Z}^*, \cdot)$ donc $[\bar{3}]^6 = [1]$

et $|[x]| = 12$.

c) $\bar{b}=\bar{6} \Rightarrow A$ n'est pas un corps

$$x^2+\bar{6} = x^2-\bar{1} = (x-\bar{1})(x+\bar{1}) = (x+\bar{1})(x+\bar{6})$$

Donc $p(x)(x-\bar{1}) \in (x^2+\bar{6}) \Leftrightarrow x+\bar{1} \mid p(x)$

$\Rightarrow \bar{a}(x+\bar{1})$ avec $\bar{a} \in \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ sont des diviseurs de zéro. De la même façon $\bar{a}(x+\bar{6})$ avec $\bar{a} \in \mathbb{Z}/72\mathbb{Z}^*$ est un diviseur de zéro. Il s'agit de la liste complète.

d) Si $\bar{b} = \bar{3}, \bar{5}, \bar{6}$ alors $x^2+\bar{b}$ est le produit de deux polynômes distincts de $\mathbb{Z}/72\mathbb{Z}[x]$ (voir tableau des carrés)

$x^2+\bar{3} = (x+\bar{5})(x+\bar{2})$

$x^2+\bar{5} = (x+\bar{3})(x+\bar{4})$

$x^2+\bar{6} = (x+\bar{6})(x+\bar{1})$

donc $x^2+\bar{b} = (x-\bar{a}_1)(x-\bar{a}_2)$

$$\frac{\mathbb{Z}/7\mathbb{Z}[x]}{((x-\bar{a}_1)(x-\bar{a}_2))} = \frac{\mathbb{Z}/7\mathbb{Z}[x]}{(x-\bar{a}_1)\cap(x-\bar{a}_2)} \simeq \frac{\mathbb{Z}/7\mathbb{Z}[x]}{(x-\bar{a}_1)} \times \frac{\mathbb{Z}/7\mathbb{Z}[x]}{(x-\bar{a}_2)}$$

$\uparrow$ car $x-\bar{a}_1$ et $x-\bar{a}_2$ sont premiers entre eux

$\uparrow$ Lemme Chinois applicable car $(x-\bar{a}_1)+(x-\bar{a}_2)$

$(x-\bar{a}_1, x-\bar{a}_2) = \mathbb{Z}/7\mathbb{Z}[x]$

Le morphisme $\mathbb{Z}/7\mathbb{Z}[x] \longrightarrow \mathbb{Z}/7\mathbb{Z}$ $\quad i=1,2$

$p(x) \longmapsto p(\bar{a}_i)$

est un morphisme surj. d'anneau de noyau $(x-\bar{a}_i)$

Le théorème d'isomorphisme nous donne donc $\frac{\mathbb{Z}/7\mathbb{Z}[x]}{(x-\bar{a}_i)} \simeq \mathbb{Z}/7\mathbb{Z}$.

Exo 3

(a) $a \in A = A_1 \times A_2$ (= (a_1, a_2)) est inversible $\Leftrightarrow \exists\, b = (b_1, b_2)$ et

$ab = (1,1)$ (= (a_1b_1, a_2b_2)) Donc a est inversible $\Leftrightarrow a_1, a_2$ sont inversibles

(b) Soit A un anneau commutatif et I, J deux idéaux t.p.

$I + J = A$ Alors on a un isomorphisme d'anneaux.

$$A/_{I\cap J} \simeq A/_I \times A/_J .$$

(c) $m \wedge n = 1 \Rightarrow \begin{cases} m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z} \\ m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z} \end{cases}$

donc $\mathbb{Z}/_{mn\mathbb{Z}} \simeq \mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}}$ est un isomorphisme d'anneaux. Or tout isomorphisme d'anneaux envoye les inversibles sur les inversibles (car l'image de l'inverse est l'inverse de l'image). Or $\mathbb{Z}/_{k\mathbb{Z}}$ a $\varphi(k)$ elements inversibles ($\forall k \in \mathbb{N}$)

Donc à cause de cal on a

$$\varphi(m)\varphi(n) = \varphi(mn).$$

Exo 4

(a) Soit G un gp fini et $H \subset G$.
On définit une relation d'equivalence sur G, R_H, par

$$g_1 R_H g_2 \iff g_1^{-1} g_2 \in H$$

les classes pour cette relation sont les classes à gauches gH $g \in G$. En plus, $\forall g \in G$, l'application $\varphi_g : H \to H$, $h \mapsto gh$

est bijective et donc $|H| = |gH|$, $\forall g \in G$

Puisque $G = \bigsqcup_g gH$ (partition de G car R_H est une relation d'equivalence)

on a $|G| = m|H|$ si m est le nombre de classe

On a démontré :

Théorème Soit G un gp fini et soit H un sous-gp de G

alors $|H| \mid |G|$

(b) Soit $1 \neq g \in G$ alors $\langle g \rangle \neq \{1\}$ et $\langle g \rangle \leq G$

le théorème de Lagrange donne $1 \neq |\langle g \rangle| \mid p = $ n° premier

donc $|\langle g \rangle| = p$ et $G = \langle g \rangle$.

(c) $H \leq S_6$ $|H| = 3$ $\Leftrightarrow$ $H = \langle g \rangle$ $\exists\, g \in S_6$ $|g| = 3$

On a deux type d'éléments d'ordre 3 dans S_6

- les 3-cycles $(a\,b\,c)$: il y en a $\binom{6}{3} 2 = 40$

- le produit de 2 3-cycles $(abc)(def)$: il y en a $\frac{1}{2}\frac{(6\cdot5\cdot4)}{3}\frac{(3\cdot2\cdot1)}{3}$ disjoints

[En effet : $(a\,b\,c)(d\,e\,f)$ — 3 choix, 2 choix, 1 choix ; 6 choix, 5 choix, 4 choix

en plus $(abc) = (bca) = (cab)$ donc on doit diviser par 3

$(def) = (efd) = (fde)$ donc on doit diviser par 3

pour finir $(abc)(def) = (def)(abc)$ donc on doit diviser par 2]

On a donc 90 éléments d'ordre 3.

Si g_1 et g_2 sont deux éléments d'ordre 3 on a

$$\langle g_1 \rangle = \langle g_2 \rangle \iff g_2 = g_1^{\pm 1}$$

car $\langle g_1 \rangle = \{1, g_1, g_1^2 = g_1^{-1}\}$ et $|g_1^{-1}| = |g_1| = 3$

Donc on a $\frac{80}{2} = 40$ sous-gps de cardinal 3.

(d) $H \leq G$ H est distingué si $\forall g \in G$ on a $gHg^{-1} = H$

Soit $H = \begin{cases} \langle (abc) \rangle \\ \langle (abc)(def) \rangle \end{cases}$ un sous-gp de cardinal 3 de S_6

Alors si $g = (ad)$ on a

$$gHg^{-1} = \begin{cases} \langle (dbc) \rangle \\ \langle (dbc)(aef) \rangle \end{cases} \neq H.$$

Donc aucun sous-gp de card. 3 est distingué dans S_6.