Corrigé

Ex1 1) Si $K[X]/(P)$ est un corps, montrons que P est irréductible par l'absurde : si P se factorisait sous la forme $P = P_1 P_2$ avec $\deg P_1 < \deg P$ et $\deg P_2 < \deg P$, alors dans $K[X]/(P)$ on aurait $\overline{P} = \overline{0} = \overline{P_1}\,\overline{P_2}$ avec $\overline{P_1} \neq 0$ et $\overline{P_2} \neq 0$. Ceci contredirait l'intégrité de $K[X]/(P)$.

Réciproquement, si P est irréductible, montrons que $K[X]/(P)$ est un corps. Soit $\overline{A}$ un élément non nul de $K[X]/(P)$. $\overline{A} \neq 0$ implique que $P \nmid A$. Comme P est irréductible, P et A sont premiers entre eux et donc il existe une relation de Bezout $PU + AV = 1$ avec $U, V \in K[X]$. Mais alors $\overline{V} \in K[X]/(P)$ est un inverse de $\overline{A}$ dans $K[X]/(P)$.

2) Soit A un anneau factoriel et $K = \mathrm{Frac}(A)$ son corps des fractions. Le critère d'Eisenstein est :

Soit $P \in A[X]$ un polynôme, $P = p_n X^n + \dots + p_0$, et soit p un élément premier de A tq $p \mid p_0, \dots, p \mid p_{n-1}$, $p \nmid p_n$, $p^2 \nmid p_0$

Alors P est irréductible dans $K[X]$.

Pour $A = \mathbb{Z}[Y]$ (qui est factoriel par le Th de Gauss) et $p = Y - 1$ qui est irréductible car de degré 1 et de contenu 1, on peut appliquer le critère d'Eisenstein à $P = Y X^n + (Y^n - 1)$. On a bien $Y-1 \mid Y^n - 1$ et $(Y-1)^2 \nmid (Y^n - 1)$ car $(Y^n - 1)' = n Y^{n-1}$ donc $Y^n - 1$ a ses racines simples.

3) On a par définition $K(a^2) \subset K(a)$.

Par le lemme de la base télescopique pour $K \subset K(a^2) \subset K(a)$ on a $\big[K(a) : K\big] = \big[K(a) : K(a^2)\big] \cdot \big[K(a^2) : K\big]$.

Or, a^2 est algébrique sur $K(a)$ puisqu'il est racine de $T^2 - a^2$. ($\in K(a^2)[T]$).
D'où $[K(a) : K(a^2)] \leq 2$ et donc soit $[K(a) : K(a^2)] = 2$ soit $K(a) = K(a^2)$.
Comme $[K(a) : K]$ est impair, on a $K(a) = K(a^2)$.

Ex 2 1) on a $\overrightarrow{AB} = \overrightarrow{DC} \iff \overrightarrow{AD} + \overrightarrow{DB} = \overrightarrow{DB} + \overrightarrow{BC}$ (par la relation de Chasles).
$\iff \overrightarrow{AD} = \overrightarrow{BC}$

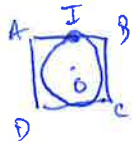
2) $GA(P)$ est $\{ f : P \to P$, affines tq $\vec{f}$ est inversible $\}$.

3) si $ABCD$ est un parallélogramme non aplati,
$\overrightarrow{AB} = \overrightarrow{DC}$ et donc $\overrightarrow{f(A)f(B)} = \vec{f}(\overrightarrow{AB}) = \vec{f}(\overrightarrow{DC}) = \overrightarrow{f(D)f(C)}$
Ceci montre que $f(A)f(B)f(C)f(D)$ est un parallélogramme.
De plus, comme $\overrightarrow{AB}$ et $\overrightarrow{AD}$ sont non colinéaires, ils forment une base de $\vec{P}$, et comme $\vec{f}$ est inversible, $\vec{f}(\overrightarrow{AB})$ et $\vec{f}(\overrightarrow{AD})$ forme aussi une base de $\vec{P}$ et donc $f(A)f(B)f(C)f(D)$ est bien non aplati.

4) Si $A_1B_1C_1D$ est un parallélogramme non aplati, (ABD) est un repère affine du plan P. Il existe une unique application du groupe affine envoyant un repère affine sur un autre.
Soit donc f tq $f(A_1) = A_2$, $f(B_1) = B_2$ et $f(D_1) = D_2$.

Mq $f(C_1) = C_2$.
On a $\overrightarrow{f(A_1)f(B_1)} = \vec{f}(\overrightarrow{A_1B_1}) = \vec{f}(\overrightarrow{D_1C_1}) = \overrightarrow{f(D_1)f(C_1)} = \overrightarrow{D_2f(C_1)}$.
$\overrightarrow{D_2C_2} = \overrightarrow{A_2B_2}$
D'où $\overrightarrow{D_2C_2} = \overrightarrow{D_2f(C_1)}$ et donc $C_2 = f(C_1)$.

5) si $ABCD$ est un carré, soit I le milieu de $[AB]$. le cercle de centre O (le centre du carré) et de rayon OI est tangent aux 4 côtés du carré en leur milieu.



Dans le cas général :
Soit f une application affine envoyant un carré sur le parallélogramme ABCD. Alors f envoie le cercle inscrit dans le carré sur une ellipse.
Comme f est affine. De plus, f préserve les milieux des côtés (car préserve les barycentres) et préserve la tangence (car f est C^1). Ainsi l'ellipse image est tangente aux côtés du parallélogramme en leurs milieux.

Ex3 : 1) Le groupe $(\mathbb{F}_q^*, \times)$ est de cardinal $q-1$.
et tout élément de $\mathbb{F}_q^*$ vérifie donc $x^{q-1} - 1 = 0$.
Ainsi tous les éléments de $\mathbb{F}_q^*$ sont racine de A.
Comme $\deg A = q-1 = |\mathbb{F}_q^*|$, on a trouvé toutes les racines et

$$A = \prod_{\alpha \in \mathbb{F}_q^*} (X - \alpha)$$ (car les deux polynômes sont unitaires)

2) Si $q \geq 3$ La somme $\sum_{\alpha \in \mathbb{F}_q} \alpha^2 = \sum_{\alpha \in \mathbb{F}_q^*} \alpha^2 = \left(\sum_{\alpha \in \mathbb{F}_q^*} \alpha\right)^2 - \sum_{\alpha \neq \beta \in \mathbb{F}_q^*} \alpha\beta$.

Par les relations coefficients-racine dans A,
$-\sum_{\alpha \in \mathbb{F}_q^*} \alpha$ est le coefficient de X^{q-2} dans A.
$\sum_{\alpha \neq \beta} \alpha\beta$ ——— X^{q-3} dans A.

Si $q > 3$, ces deux coefficients sont nuls et donc $\sum_{\alpha \in \mathbb{F}_q} \alpha^2 = 0$.

Si $q = 2$, $\sum_{\alpha \in \mathbb{F}_2} \alpha^2 = 1$ et si $q = 3$, $\sum_{\alpha \in \mathbb{F}_3} \alpha^2 = 2$.

Ex 4 1) Si Q est irréductible alors $k[X]/(Q)$ est un corps de rupture et si L est une extension de k contenant une racine α de Q, alors $j : k[X]/(Q) \to L$, $X \mapsto \alpha$ est un morphisme de corps et $\mathrm{im}(j)$ est un sous-corps de L isomorphe à $k[X]/(Q)$.

En particulier, $[L:k] = [L:\mathrm{im}(j)]\,[\mathrm{im}j : k]$ montre que $[L:k] \geq n$ ($[\mathrm{im}j : k] = n$).

Réciproquement si Q est réductible, $\exists\, Q_1, Q_2$ tq $Q = Q_1 Q_2$ avec $\deg Q_1 \leq \frac{n}{2}$. et alors Q a une racine dans le corps $k[X]/(Q_1)$ qui est une extension de k de degré $\deg Q_1$ (et Q_1 irréductible).

2) Si Q est de degré 4 sur $\mathbb{F}_p$ et irréductible, alors Q n'a pas de racine dans $\mathbb{F}_{p^2}$ qui est une extension de $\mathbb{F}_p$ de degré 2.

Par contre Q a une racine dans $\mathbb{F}_{p^4} = \mathbb{F}_p[X]/(Q)$ qui est une extension de degré 2 de $\mathbb{F}_{p^2}$, donc Q vu comme polynôme de $\mathbb{F}_{p^2}[X]$ a une racine dans une extension de degré 2 et n'est donc pas irréductible.

Comme $Q \in \mathbb{F}_{p^2}[X]$ n'a pas de racine dans $\mathbb{F}_{p^2}$, les facteurs de Q sont nécessairement irréductibles de degré 2.

Réciproquement, si $Q = Q_1 Q_2$ dans $\mathbb{F}_{p^2}[X]$, avec Q_1 et Q_2 irréductibles, alors Q n'a pas de racine dans $\mathbb{F}_{p^2}$ qui est la seule extension de degré 2 de $\mathbb{F}_p$ et donc par a), Q est irréductible sur $\mathbb{F}_p[X]$.