Ex 1.

1. discrete $\Rightarrow \forall v \in L \ \exists r_v > 0 \quad B_{r_v}(v) = \{v\}$
   assume $\exists v \in L : v' \in B_{r_0}(v) \setminus \{v\}$, i.e. $\|v - v'\| < r_0$
   $\Rightarrow \quad v' - v \neq 0$ but $v - v' \in B_{r_0}(0)$ ↯
2. $a_n \to a \in L$
   def $\Rightarrow \forall \varepsilon > 0 \ \exists N_\varepsilon \in \mathbb{N} \ \forall n \geq N_\varepsilon : \|a_n - a\| \leq \varepsilon$
   1 $\Rightarrow \exists r : B_r(a) = \{a\}$
   but $\forall n \geq N_r : a_n \in B_r(a) \Rightarrow a_n = a$
3. · $B_r(\vec{v})$ can be covered with finite number of balls of radius $s/2$, where s is the radius of Q1.
   · per such ball, at most 1 lattice point
   $\Rightarrow$ statement
4. $f : \mathbb{N} \to L$, $f(n)$ defined as follows
   · let $r \in \mathbb{N}$ minimal s.t. $\sum_{i=1}^{r} |B_r(0) \cap L| < n$
   · output n-th element in $(B_r(0) \setminus B_{r-1}(0)) \cap L$ (which is finite, so countable)
   · clearly f is surjective

Ex 2:

discrete $\Rightarrow$ 1. $\overset{\text{Ex1.}}{\Rightarrow}$ 2.
we show "2. $\Rightarrow$ discrete", i.e. not discrete $\Rightarrow \exists$ injective sequence conv. to 0
not discrete: $\exists v \in L \ \forall r > 0 : |B_r(v)| \geq 2$
let $a_0 \in B_1(v) \setminus \{v\}$
$a_n \in B_{\|v - a_{n-1}\|/2}(v) \setminus \{v\}$
let $s_n = v - a_n$
$s_n \to 0$ but s_n injective

Ex 3.

1. clear
2. clear
3. closed: $\sum x_i b_i + \sum y_i b_i = \sum (x_i + y_i) b_i$
4. closed as above, discrete:
   assume $\exists a_n \to 0$ in L
   $\Rightarrow a_n = \sum x_{i,n} b_i \to 0$
   but $\lim x_{i,n} \in \mathbb{R}$ ↯ linear independence

Ex 4:

1. if $f = 0$, then $v = 0$

else take some basis B, have for $w \in L$: $w = B \cdot x$

write $f(w) = \sum_i x_i f(b_i)$

set v as unique solution of

$$v^t B = (f(b_1), .., f(b_k))^t \qquad \text{(exists bc } B \text{ is full rank)}$$

Thus:

$$\begin{aligned} f(w) &= \sum x_i f(b_i) \\ &= (f(b_1), \dots, f(b_k))^t \cdot x, \quad \text{where } x = (x_1, .., x_k) \in \mathbb{Z}^k \\ &= v^t B \cdot x \\ &= v^t w = \langle v, w \rangle \end{aligned}$$

2. close clear, assume $\exists \vec{v}_i \in L^\times : \vec{v}_i \to 0$

then $\underbrace{\langle v_i, b_j \rangle}_{\in \mathbb{Z}} \to 0 \quad \forall b_j$ in basis of L

$\Rightarrow$ v_i is stationary

3. set $\Phi : \{f : L \to \mathbb{Z}\} \to L^\times, \; f \mapsto \vec{v}_f$ (from Q1)

$$\begin{aligned} (f_1 + f_2)(x) &= f_1(x) + f_2(x) \\ &= \vec{v}_{f_1} + \vec{v}_{f_2} \in L^\times \end{aligned}$$

as $\langle v_{f_1} + v_{f_2}, w \rangle = \langle v_{f_1}, w \rangle + \langle v_{f_2}, w \rangle \in \mathbb{Z} \quad \forall w \in L$

- surjective: $\langle v, . \rangle$ for $v \in L^\times$ maps to v
- $\ker(\Phi) = 0$ bc. $\langle v, w \rangle = 0 \quad \forall w \in L$ iff $v = 0$

Ex 5.

1. $P+P=0 \Rightarrow P=-P$. $-P=-(x,y)=(x,-y)$

$\Rightarrow -y=y \Rightarrow y=0$

$y=0 \Rightarrow P+P=\mathcal{O}$

2. all such points are roots of f.

→ 3 roots and neutral element $\mathcal{O}$.

(f non-singular → no double roots)

3. $3P=0 \Rightarrow 2P=-P$

$\overset{Q1}{\Rightarrow} x(P)=x(-P) \Rightarrow x(2P)=x(P)$

$x(2P)=x(P) \Rightarrow 2P=P$ or $2P=-P$ (as at most 2 points on C with same x-coordinate)

But $[2P=P \Rightarrow P=\mathcal{O})$, so $2P=-P$

4.

$x(P)=x=x(2P)$. identity yields $\psi_3(x)=0$

1. *On a :* $\|\vec{u} - q\vec{v}\|^2 = \|\vec{u}\|^2 - 2q\langle\vec{u},\vec{v}\rangle + q^2\|\vec{v}\|^2$. *Son minimum sur* $\mathbb{R}$ *est donc atteint en* $q_0 = \frac{\langle\vec{u},\vec{v}\rangle}{\|\vec{v}\|^2}$. *Or* $q = q_0$ *est un axe de symétrie de cette parabole, donc le minimum sur* $\mathbb{Z}$ *est atteint en* $\lfloor q_0 \rceil$. *Cette question montre que l'algorithme de Lagrange est glouton. Attention, contrairement à ce que plusieurs personnes ont sous-entendu : si une fonction* f *admet un minimum sur* $\mathbb{R}$ *en* x_0, *son minimum sur* $\mathbb{Z}$ *n'est pas nécessairement en* $\lfloor x_0 \rceil$. *Ici, c'est vrai parce que* f *est une fonction polynomiale du second degré.*

2. *On remarque tout d'abord un invariant de boucle :* $(\vec{u},\vec{v})$ *est une base de* L. *Si la boucle de l'étape 8 ne s'arrête pas, c'est que* $\|\vec{u}\| > \|\vec{v}\|$, *et il existe alors une suite de vecteurs du réseau dont la norme est strictement décroissante et non nulle car chaque* $(\vec{u},\vec{v})$ *est une base de* L. *Or on a vu en cours que l'intersection d'un réseau avec une boule est finie : contradiction.*

3. — *Si* $q = 0$, *les étapes 5 à 8 ne font qu'échanger* $\vec{u}$ *et* $\vec{v}$. *Or on remarque qu'au début de chaque itération de boucle, on a* $\|\vec{u}\| \geq \|\vec{v}\|$. *En effet, c'est vrai pour la première itération de boucle à cause des trois premières lignes. Et c'est vrai aussi pour les autres itérations à cause de la condition de sortie à la ligne 8. Donc, après échange, on a forcément* $\|\vec{u}\| \leq \|\vec{v}\|$, *donc la boucle s'arrête : c'est bien la dernière itération.*
   — *Si* $|q| = 1$ *et que ce n'est pas la dernière itération, on a* $\|\vec{u}\hat{A} + q\vec{v}\| < \|\vec{v}\|$. *Comme* $q = \pm 1$, *on en déduit que* $\min_{q'\in\mathbb{Z}} \|q'\vec{u}\hat{A} + \vec{v}\| < \|\vec{v}\|$, *ce qui ne peut arriver qu'à la première itération, car l'algorithme est glouton : pour toute itération qui n'est pas la première,* $\vec{v}$ *ne peut être raccourci en lui soustrayant un multiple de* $\vec{u}$.

4. *On en déduit que pour toute itération qui n'est ni la première, ni la dernière, on a* $|q| \geq 2$. *Donc* $|\mu| \geq \frac{3}{2}$ *où* $\mu = \frac{\langle\vec{u},\vec{v}\rangle}{\|\vec{v}\|^2}$. *Or* $\vec{u} = \mu\vec{v} + \vec{w}$ *avec* $\vec{w}$ *la projection orthogonale de* $\vec{u}$ *sur l'hyperplan* $\vec{v}^\perp$. *Donc* $\|\vec{u}\|^2 = \mu^2\|\vec{v}\|^2 + \|\vec{w}\|^2 \geq \frac{9}{4}\|\vec{v}\|^2 + \|\vec{w}\|^2$. *Donc* $\|\vec{v}\|^2 \leq \frac{4}{9}\hat{A}\ \|\vec{u}\|^2$. *Mais comme ce* $\vec{v}$ *n'est autre que le prochain* $\vec{u}$, *on en déduit qu'à chaque itération, sauf éventuellement les deux premières et la dernière,* $\|\vec{u}\|^2$ *va diminuer d'un facteur mutiplicatif* $\geq \frac{9}{4}$. *On conclut puisque* $\|\vec{u}\| \geq \lambda_1(L)$ *car* $\vec{u} \neq 0$ *puisque* $(\vec{u},\vec{v})$ *est toujours une base.*

5. *Soit* $M = \max(\|\vec{u}\|, \|\vec{v}\|)$ *au début de l'algorithme de Lagrange. On remarque l'invariant de boucle :* $\|\vec{u}\| \leq M$ *et* $\|\vec{v}\| \leq M$, *donc chaque opération de l'algorithme est polynomiale en* $\log M$. *Or il y a un nombre polynomial d'itérations de boucle, donc l'algorithme de Lagrange est polynomial. Une analyse plus précise montre qu'on peut implémenter l'algorithme de Lagrange en temps quadratique, en utilisant l'algorithme de division euclidienne usuel, sans utiliser de transformée de Fourier.*