SÉMINAIRE DE THÉORIE DES NOMBRES DE BORDEAUX

JACQUES VÉLU

Quelques aspects de la théorie des courbes elliptiques

Séminaire de théorie des nombres de Bordeaux (1970-1971), exp. n° 20, p. 1-13

<http://www.numdam.org/item?id=STNB_1970-1971____A20_0>

Séminaire de Théorie des Nombres
Année 1970-1971 , exposé n° 22

QUELQUES ASPECTS DE LA THEORIE DES COURBES ELLIPTIQUES

par

Jacques VÉLU

-:-:-:-

I. - RAPPELS [1]

I. 1. - Modèles

I. 1. 1. - Soit E une courbe elliptique définie sur un corps k , munie d'un point rationnel sur k . Alors E admet un modèle non-singulier du type :

$$(1) \qquad y^2t + a_1xyt + a_3yt^2 = x^3 + a_2x^2t + a_4xt^2 + a_6t^3 \ , \text{ avec } a_i \in k \ .$$

Remarques :

1) Ce modèle associé à E n'est pas unique, les autres s'en déduisent par des transformations du type

$$(2) \qquad (u, a, b, c) \begin{cases} x \mapsto u^2x' + a \\ y \mapsto u^3y' + u^2bx' + c \end{cases}$$

où $u \in k^\times$ a, b, c $\in$ k .

2) L'étude des variétés abéliennes de dimension 1 sur k se ramène donc à l'étude des cubiques non-singulières du type (1).

I. 1. 2. - Discriminant. Il faut savoir reconnaître si une cubique du type (1) est non singulière. Pour cela, on définit le discriminant Δ par les formules suivantes :

$$
\begin{aligned}
&b_2 = a_1^2 + 4a_2 \qquad && c_4 = b_2^2 - 24b_4 \\
&b_4 = a_1a_3 + 2a_4 \qquad && c_6 = -b_2^3 + 36b_2b_4 - 216\,b_6 \\
&b_6 = a_3^2 + 4a_6 \\
&b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2 \\
&\Delta = -b_2^8b_8 - 8b_4^3 - 27\,b_6^2 + 9\,b_2b_4b_6
\end{aligned}
\tag{3}
$$

et on a les relations :

$$4b_8 = b_2b_6 - b_4^2 \qquad 1\,728\,\Delta = c_4^3 - c_6^2 .$$

THEOREME. La cubique (1) est non-singulière si et seulement si Δ est non nul.

De plus un changement de modèle du type (u, a, b, c) change Δ en $\Delta' = u^{-12}\Delta$.

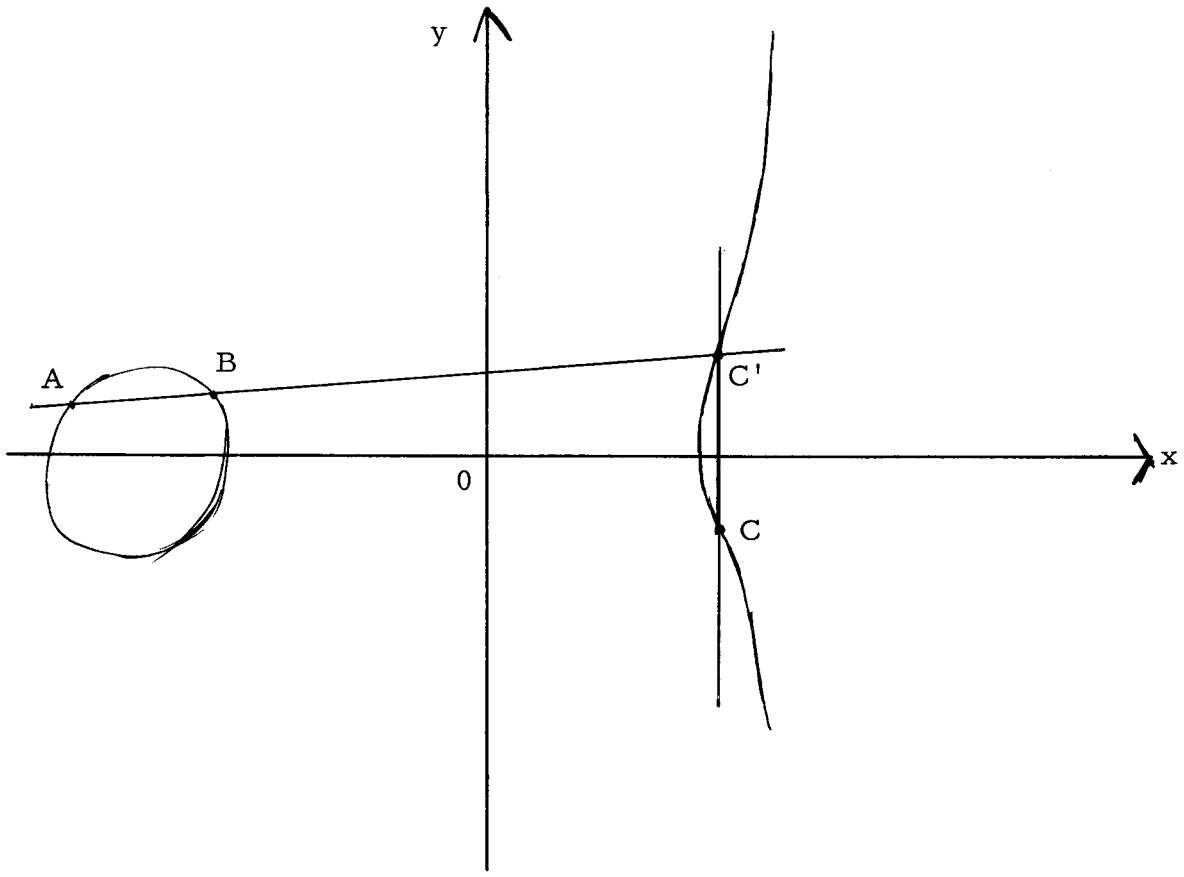
I. 2. - Loi de groupe abélien

Sur une cubique du type (1) on montre que les conditions suivantes définissent une loi de groupe abélien :

(4)
(i) l'unique point à l'infini $0 = (0, 1, 0)$ est élément neutre

(ii) $A + B + C = 0 \Leftrightarrow$ A, B, C alignés.

On peut faire un dessin pour rendre plus claire la construction de $A + B = C$.



Supposons que $C + C' = 0$, alors C, C' et 0 sont alignés, ce qui signifie que C et C' sont sur une parallèle à $0y$; d'où la construction de C'.

Maintenant, la droite (AB) recoupe E en C'. On a $A + B + C' = 0$ et $C + C' = 0$, donc

$$A + B = C$$

et on a la construction de $A + B$.

On peut donner des formules permettant de calculer les coordonnées de C en fonction de celles de A et B.

L'équation affine de E est :

$$y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 . \qquad (5)$$

Soit $C\ (x_3, y_3)$, alors C' est sur la parallèle à $0y$ passant par C

(6) $\quad C'(x_3\ ,\ -y_3 - a_1x_3 - a_3)\ .$

Maintenant considérons $A(x_1, y_1)$ et $B(x_2, y_2)$. La droite (A B) a pour équation :

$$Y = mX + c\ ,\quad \text{où :}$$

(7)
$$\begin{cases} m = \dfrac{y_2 - y_1}{x_2 - x_1} & \text{si } A \neq B \\ m = \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \text{si } A = B\ , \text{ et} \\ c = y_1 - mx_1\ . \end{cases}$$

En remplaçant Y par $mX + c$ dans (5) et en ordonnant en X, on trouve :

$$X^3 + X^2(a_2 - m^2 - a_1m) + \ldots . = 0$$

on a donc $\quad x_1 + x_2 + x_3 = -a_2 + m^2 + a_1 m$

et $\quad x_3 = -x_1 - x_2 - a_2 + m^2 + a_1m\ .$

On recommence en remplaçant X par $\dfrac{Y-c}{m}$ dans (5)

$$\frac{Y^3}{m^3} + Y^2\left(\frac{a_2}{m^2} - \frac{3c}{m^3} - \frac{a_1}{m} - 1\right) + \ldots = 0\ ,$$

on a donc $\quad y_1 + y_2 + y'_3 = 3c + m^3 + a_1m^2 - a_2m$

et $\quad y'_3 = -y_1 - y_2 + 3c + m^3 + a_1m^2 - a_2m\ .$

En résumé :

(8)
$$\begin{cases} (x_1, y_1) + (x_2, y_2) = (x_3, y_3)\ , & \text{avec} \\ x_3 = -x_1 - x_2 + m^2 + a_1m - a_2 & \\ y_3 = y_1 + y_2 - 3c + a_2m - m^3 - a_1m^2 - a_1x^3 - a_3\ , & \text{et} \\ (x_3, y_3) + (x_3, y'_3) = 0\ , & \text{avec} \\ y'_3 = -y_3 - a_1x_3 - a_3\ . & \end{cases}$$

I. 3. - Groupe des points rationnels

Soit K une extension quelconque de k . On note E(K) l'ensemble des points de E définis sur K . Comme les formules (8) sont à coefficients dans k , l'ensemble E(K) est ainsi muni d'une loi de groupe abélien.

I. 4. - Endomorphismes

Soit K une extension de k . On note $\mathrm{End}_K(E)$ les couples (P, Q) tels que :

$$(9)\quad \begin{cases} \text{(i)} & P \text{ et } Q \in K(X_1, X_2) \\ \text{(ii)} & \text{si } x' = P(x,y) \text{ et } y' = Q(x,y) \\ & \text{alors } (x,y) \in E \Rightarrow (x',y') \in E \\ \text{(iii)} & \text{si } (x_3, y_3) = (x_1, y_1) + (x_2, y_2) \\ & \text{alors } (x'_3, y'_3) = (x'_1, y'_1) + (x'_2, y'_2) \end{cases}$$

$\mathrm{End}_K(E)$ forme un anneau dans lequel Z se plonge de la façon suivante :

$$(10)\quad \begin{cases} \text{pour} \quad n > 0 & [n](x,y) = \underbrace{(x,y) + \ldots + (x,y)}_{n \text{ fois}} \\ \text{et} & [-1](x,y) = (x, -y - a_1 x - a_3) \end{cases}$$

De plus si L est une sous-extension de K , $k \subset L \subset K$, $\mathrm{End}_L(E)$ opère sur le groupe E(K) .

II. - COURBES ELLIPTIQUES SUR LES CORPS FINIS [2], [3]

Nous nous limiterons aux courbes elliptiques définies sur $k = \mathbf{F}_p$.

II. 1. - Points d'ordre ℓ (ℓ premier)

On montre que les points d'ordre ℓ sont définis sur $\overline{\mathbf{F}}_p$ (clôture algébrique de $\mathbf{F}_p$) donc forment un sous-groupe E_ℓ de $E(\overline{\mathbf{F}}_p)$. On a le

résultat :

$$(11)\quad \begin{cases} \text{si } \ell \neq p \quad E_\ell \simeq \mathbb{Z}/\ell \times \mathbb{Z}/\ell \\ \text{si } \ell = p \begin{cases} \text{ou } E_p \simeq \mathbb{Z}/p & \text{on dit que hauteur de } E \text{ , } ht(E) = 1 \\ \text{ou } E_p \simeq \{0\} & \text{on dit que } ht(E) = 2. \end{cases} \end{cases}$$

II. 2. - Endomorphismes

On montre que les endomorphismes sont tous définis sur la clôture algébrique de $\mathbb{F}_p$. On considère donc $\mathrm{End}_{\overline{\mathbb{F}}_p}(E)$. Il y a deux possibilités

$$(12)\quad \begin{cases} ht\, E = 1 \Leftrightarrow \mathrm{End}_{\overline{\mathbb{F}}_p}(E) & \text{est isomorphe à un ordre d'un corps quadratique imaginaire.} \\ ht\, E = 2 \Leftrightarrow \mathrm{End}_{\overline{\mathbb{F}}_p}(E) & \text{est isomorphe à un ordre maximal de l'unique corps de quaternions ramifié uniquement en } p \text{ et } \infty . \end{cases}$$

Conséquences :

1) En identifiant $\mathbb{Z}$ à son image dans $\mathrm{End}_{\overline{\mathbb{F}}_p}(E)$ tout endomorphisme vérifie une équation du type :

$$(13)\qquad \varphi^2 - a\varphi + b = 0 \qquad \text{avec} \qquad a \text{ et } b \in Z$$

(ce qui signifie $\varphi \circ \varphi - [a] \circ \varphi + [b] = 0$) .

Ce qui permet de définir la norme de φ et la trace de φ par

$$(14)\quad \begin{cases} N(\varphi) = b \\ Tr(\varphi) = a \end{cases}$$

2) Tout endomorphisme qui n'est pas du type $[n]$ se plonge dans $\mathbb{C}$ et non pas dans $\mathbb{R}$, d'où les inégalités

$$(15)\qquad N(\varphi) \geq 0 \qquad \text{et} \qquad |Tr(\varphi)| \leq 2\sqrt{N(\varphi)} .$$

On démontre le théorème suivant (en utilisant un peu de géométrie algébrique) :

THEOREME. Pour tout $\varphi \in \mathrm{End}_{\mathbb{F}_p}(E)$, $N(\varphi) = \#\,\mathrm{Ker}(\varphi)$ ($\#$ signifie cardinal).

II. 3. - Endomorphisme de Frobenius

Les formules (8) étant définies sur $\mathbb{F}_p$, l'application

(17) $\pi : (x, y) \mapsto (x^p, y^p)$ est un endomorphisme ;

on l'appelle l'endomorphisme de Frobenius de la courbe.

Nous pouvons appliquer ce qui précède à π.

Nous avons :

(18) $N(\pi) = p$

(l'idée de la démonstration est que $\mathrm{Ker}\ \pi$ est l'élément neutre compté p fois).

De plus, $(x, y) \in \mathrm{Ker}(\pi - 1) \Leftrightarrow x^p = x$ et $y^p = y$,

donc $\#\,\mathrm{Ker}(\pi - 1) = \#\,E(\mathbb{F}_p)$.

Mais $N(\pi - 1) = N(\pi) - \mathrm{Tr}(\pi) + 1$,

donc si nous posons

$$A = \#\,E(\mathbb{F}_p),$$

nous avons

$$(19) \quad \begin{cases} A = p - \mathrm{Tr}(\pi) + 1 \quad , \quad \text{ou encore} \\ \mathrm{Tr}(\pi) = p - A + 1 \ . \end{cases}$$

Comme il est facile de calculer A, il est facile de calculer $\mathrm{Tr}(\pi)$.

L'inégalité (15) montre que :

$$(20) \quad \begin{cases} |p+1-A| \leq 2\sqrt{p} \quad , \quad \text{ou encore} \\ p+1-2\sqrt{p} \leq A \leq p+1+2\sqrt{p} \ . \end{cases}$$

Remarques : 1) L'inégalité (20) s'appelle parfois "hypothèse de Riemann".

2) J. Tate a montré que pour tout entier A vérifiant (20), il existe une courbe elliptique E définie sur $\mathbf{F}_p$ telle que $A = \#\, E(\mathbf{F}_p)$.

3) Les endomorphismes définis sur $\mathbf{F}_p$ sont ceux qui commutent avec π. Donc si $ht(E) = 1$, tout endomorphisme est défini sur $\mathbf{F}_p$.

4) On montre que pour que $ht(E) = 2$, il faut et il suffit que $Tr(\pi) \equiv 0\ (p)$ ce qui joint à (20) montre que si $p > 3$, $ht(E) = 2 \Leftrightarrow Tr\,\pi = 0$.

Nous pouvons résumer ces résultats :

	$ht\,E = 1$ ⇕	$ht\,E = 2$ ⇕
	$E_p \simeq \mathbf{Z}/p$ ⇕	$E_p \simeq 0$ ⇕
	$End_{\overline{\mathbf{F}}_p}(E) \simeq$ ordre d'un corps quad. imag. ⇕	$End_{\overline{\mathbf{F}}_p}(E) \simeq$ ordre maximal du corps de quaternions ramifié en p et ∞ ⇕
	$End_{\overline{\mathbf{F}}_p}(E)$ est commutatif ⇕	$End_{\overline{\mathbf{F}}_p}(E)$ n'est pas commutatif ⇕
	$End_{\overline{\mathbf{F}}_p}(E) = End_{\mathbf{F}_p}(E)$ ⇕	$End_{\overline{\mathbf{F}}_p}(E) \neq End_{\mathbf{F}_p}(E)$ ⇕
	$Tr\,\pi \not\equiv 0\ (p)$ ⇕	$Tr\,\pi \equiv 0\ (p)$ ⇕
si $p > 3$	$Tr\,\pi \neq 0$ ⇕ $A \neq p + 1$	$Tr\,\pi = 0$ ⇕ $A = p + 1$

Traitons un exemple :

Considérons la courbe E définie sur $\mathbb{F}_5$ par

$$y^2 = x^3 + 1 \quad .$$

Soit $j \in \mathbb{F}_{25}$ tel que $j^2 + j + 1 = 0 \qquad (j \notin \mathbb{F}_5)$.

Il est facile de voir que

$$\varphi \begin{cases} x \mapsto jx \\ y \mapsto y \end{cases} \qquad \text{est un endomorphisme de } E .$$

$\varphi \in \mathrm{End}_{\mathbb{F}_{25}}(E)$ et $\varphi \notin \mathrm{End}_{\mathbb{F}_5}(E)$ car

$$\varphi \circ \pi (x, y) = (j x^5 , y^5)$$

$$\pi \circ \varphi (x, y) = (j^2 x^5 , y^5) \qquad \text{d'où} \quad \pi \circ \varphi \neq \varphi \circ \pi$$

par conséquent $\mathrm{ht}(E) = 2$. Un calcul direct montre que $A = 6$ et $\mathrm{Tr}\,\pi = 0$.

III. - COURBES ELLIPTIQUES SUR $\mathbb{Q}$ [1], [4]

Il est facile de voir qu'une courbe elliptique définie sur $\mathbb{Q}$ admet plusieurs modèles du type

$$(21) \qquad y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

où les $a_i \in \mathbb{Z}$ et par conséquent où $\Delta \in \mathbb{Z}$.

Un changement de modèle multiplie ou divise Δ par la puissance 12^e d'un entier. Donc le signe de Δ est inchangé. Pour une courbe donnée, il existe un Δ minimum et une infinité de modèles ayant ce discriminant.

On peut en choisir un unique en imposant par exemple

$$a_1 \in \{0, 1\}$$
$$a_3 \in \{0, 1\}$$
$$a_2 \in \{-1, 0, 1\} .$$

On l'appellera modèle canonique le discriminant minimum.

III. 1. - Si K est un corps de nombres, le théorème de Mordell-Weil dit que le groupe $E(K)$ est un $\mathbb{Z}$-module de type fini.

Le rang de $E(\mathbb{Q})$ s'appelle le rang de la courbe.

III. 2. - Endomorphismes [8]

Soit E une courbe elliptique définie sur $\mathbb{Q}$. L'anneau $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$ peut être isomorphe : - soit à $\mathbb{Z}$,

,- soit à un ordre d'un corps quadratique imaginaire, le nombre de classe de cet ordre étant 1.

Dans le premier cas, on dit que la courbe n'admet pas de multiplication complexe, dans le second qu'elle admet des multiplications complexes.

Remarque : Il y a treize ordres ayant pour nombre de classe 1.

Ce sont les anneaux engendrés par :

$$(1 \text{ et } \sqrt{-1}) \ , \ (1 \text{ et } \sqrt{-2}) \ , \ (1 \text{ et } \frac{-1+\sqrt{-3}}{2}) \ , \ (1 \text{ et } \frac{-1+\sqrt{-7}}{2}),$$

$$(1 \text{ et } \frac{-1+\sqrt{-11}}{2}) \ , \ (1 \text{ et } \frac{-1+\sqrt{-19}}{2}) \ , \ (1 \text{ et } \frac{-1+\sqrt{-43}}{2}) \ ,$$

$$(1 \text{ et } \frac{-1+\sqrt{-67}}{2}) \ , \ (1 \text{ et } \frac{-1+\sqrt{-163}}{2})$$

qui sont des ordres maximaux dans leur corps de fractions et les anneaux engendrés par

$$(1 \text{ et } 2\sqrt{-1}) \ , \ (1 \text{ et } \sqrt{-3}) \ , \ (1 \text{ et } \sqrt{-7})$$

qui ont le conducteur 2 dans leur corps de fractions et

$$(1 \text{ et } \frac{-1+3\sqrt{-3}}{2}) \quad \text{qui a le conducteur 3 dans } \mathbb{Q}(\sqrt{-3})$$

IV. - REDUCTION MODULO p [5]

Considérons une courbe E définie sur $\mathbb{Q}$ et un modèle canonique de discriminant minimal

$$(22) \qquad y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \qquad (a_i \in \mathbb{Z}) .$$

Pour tout p, soit E_p la courbe définie sur $\mathbb{F}_p$ ayant pour équation l'équation (22) réduite modulo p.

Si $p \mid \Delta$, E_p n'est pas une courbe elliptique ; c'est une cubique ayant un point double. On dit que E a mauvaise réduction en p.

Si $p \nmid \Delta$, ce qui est le cas pour presque tout p, E_p est une courbe elliptique sur $\mathbb{F}_p$; on dit que E a bonne réduction en p.

On calcule $A_p = \# E_p$ et $c_p = \mathrm{Tr}\, \pi_p$ pour tout p de bonne réduction.

On a, si l'on plonge π_p dans $\mathbb{C}$

$$\pi_p = \sqrt{p}\, e^{\pm i\theta_p} \quad \text{avec} \quad 0 \leq \theta \leq \pi$$

et
$$\mathrm{ht}(E_p) = 2 \underset{(p>3)}{\Leftrightarrow} \theta_p = \frac{\pi}{2} .$$

a) Si E a des multiplications complexes, l'ensemble des p pour lesquels $\mathrm{ht}(E_p) = 2$ a pour densité $\frac{1}{2}$.

Par exemple, si E est $y^2 = x^3 + 1$, elle admet la multiplication complexe :

$$\varphi \begin{cases} x \to jx \\ y \to y \end{cases}$$

donc
$$\mathrm{ht}(E_p) = 2 \Leftrightarrow \mathrm{End}_{\overline{\mathbb{F}}_p}(E) \text{ non commutatif}$$
$$\Leftrightarrow \pi \circ \varphi \neq \varphi \circ \pi$$
$$\Leftrightarrow j \notin \mathbb{F}_p$$
$$\Leftrightarrow p \not\equiv 1 (3)$$

et on voit bien ici, à l'aide du théorème de la progression arithmétique, que la densité des p de hauteur 2 est bien $\frac{1}{2}$.

C'est à peu près de cette façon qu'on montre le théorème dans le cas général.

b) J. P. Serre a montré que si E est sans multiplication complexe, l'ensemble des p pour lesquels $ht(E_p) = 2$ a pour densité 0.

Une question ouverte est de savoir s'il existe des courbes pour lesquelles cet ensemble est vide et dans le cas contraire quel est l'ordre de grandeur du plus petit p de l'ensemble.

c) Une autre question ouverte est la conjecture de Sato [6] qui dit que si E est sans multiplication complexe, les θ_p sont équirépartis entre 0 et π pour la mesure $\frac{2}{\pi} \sin^2\theta \, d\theta$.

d) Il y a encore de nombreuses conjectures sur les c_p les plus célèbres sont celles de Birch et Swinnerton-Dyer [7].

-:-:-:-

BIBLIOGRAPHIE

[1] CASSELS. - Diophantine equations with special reference to elliptic curves. (J. London Math. Soc., 1966).

[2] J. P. SERRE. - Cours E N S, mai 1970.

[3] DEURING. - Die typen der multiplikationringe elliptischer funktionenkorper (Ab h Math. Sem. Hamburg, 1941).

[4] J. P. SERRE. - Cours au Collège de France, 1970-71.

[5] NERON. - Modèles minimaux des variétés abéliennes sur les corps globaux. Publications math. de l'I H E S.

[6] J. P. SERRE. - Abelian ℓ-adic representations (Benjamin). Exercices du chapitre 1.

[7] BIRCH - SWINNERTON DYER. - Conjectures concerning elliptic curves. J. reine angew. Math. p. 212-218.

[8] Seminar on Complex Multiplication. (Lecture notes Springer) n° 21.

-:-:-:-

J. VÉLU
3, résidence du Parc
91 - Palaiseau