Le couplage de Weil: de la géométrie à l'arithmétique

Bas Edixhoven

le 28 février 2002

1 Cours sur le couplage de Weil dans le cadre du séminaire de cryptographie; 2002/02/11

Sur les couplages de Weil et de Tate.

Déjà, j'ai eu un problème, car je ne sais pas ce que c'est le couplage de Tate[1].

Dans cet exposé, je veux d'abord expliquer pourquoi, du point de vue de la topogie des surfaces de Riemann, on doit s'attendre à l'existence d'un couplage (ou accouplement) de Weil. Ensuite, je parlerai de quelques contructions (et des propriétés) des couplages de Weil.

1.1 Références

- Griffiths-Harris, *Principles of Algebraic Geometry*, §0.4.
- Milne, *Abelian Varieties* et *Jacobian Varieties* dans "Arithmetic Geometry" (Springer-Verlag).
- Silverman. *The arithmetic of elliptic curves.*
- Katz and Mazur. *Arithmetic moduli of elliptic curves.* Princeton University Press.
- Serre. *Groupes algébriques et corps de classes.*
- mes pages web (cours de DEA).

[1] Après l'exposé de Joux, il me semble que c'est la dualité entre les noyaux de deux isogénies duales

1.2 Le point de vue analytique complexe

Soit X une variété analytique complexe non singulière, compacte, connexe, de dimension (complexe) un. **Faire un dessin.** Localement, X est donc isomorphe à un disque ouvert dans $\mathbb{C}$. Soit g le genre de X: c'est le nombre de "trous", ou encore:

$$g = \frac{1}{2}\mathrm{rank}_{\mathbb{Z}}\mathrm{H}_1(X,\mathbb{Z}) = \dim_{\mathbb{C}}\Omega^1(X)$$

Ici, $\mathrm{H}_1(X,\mathbb{Z})$ est le premier groupe de homologie singulière de X, et aussi l'abélianisé du groupe fondamental. Les éléments de $\mathrm{H}_1(X,\mathbb{Z})$ sont donc des sommes finies $\sum_i n_i\gamma_i$ avec les n_i dans $\mathbb{Z}$ et les γ_i des lacets, à homotopie près. Dans les formules pour g, $\Omega^1(X)$ est le $\mathbb{C}$-espace vectoriel des 1-formes différentielles holomorphes sur X. Si X est une courbe elliptique $\mathbb{C}/\Lambda$, on a $\Omega^1(X) = \mathbb{C}dz$, avec z la coordonnée sur $\mathbb{C}$.

Deux choses sont très importantes maintenant.

1. $\mathrm{H}_1(X,\mathbb{Z}) \times \Omega^1(X) \longrightarrow \mathbb{C}$, $(\gamma,\omega) \mapsto \int_\gamma \omega$. Cette application est $\mathbb{C}$-linéaire en ω.

2. $\mathrm{H}_1(X,\mathbb{Z}) \times \mathrm{H}_1(X,\mathbb{Z}) \longrightarrow \mathbb{Z}$, $(\gamma_1,\gamma_2) \mapsto \gamma_1\cdot\gamma_2$, le produit d'intersection orientée. Ceci est un produit alternée: $\gamma\cdot\gamma = 0$ pour tout γ, et est un accouplement parfait: chaque facteur est identifé au dual (à valeurs dans $\mathbb{Z}$) de l'autre. Il existe donc une base de $\mathrm{H}_1(X,\mathbb{Z})$ dans laquelle le produit est donnée par la matrice (en blocs) $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$.

On peut définir alors la variété jacobienne J de X comme: $J := \Omega^1(X)^\vee/\mathrm{H}_1(X,\mathbb{Z})$. En fait, l'image de $\mathrm{H}_1(X,\mathbb{Z})$ dans $\Omega^1(X)^\vee$ est un réseau (discret et co-compact). On peut voir J comme groupe abélien, ou comme tore complexe (donc munie de sa structure de variété analytique complexe) mais en fait c'est une variété abélienne (donc provient d'une variété algébrique complexe, projective). Une interprétation utile est: $J = \mathrm{Div}^0(X)/\mathrm{div}(\mathbb{C}(X)^*)$. On va voir ça plus loin.

Pour n un entier, on note $J[n]$ le noyau de multiplication par n sur J. On a donc, pour $n \neq 0$:

$$J[n] = \frac{1}{n}\mathrm{H}_1(X,\mathbb{Z})/\mathrm{H}_1(X,\mathbb{Z}) = \mathrm{H}_1(X,\mathbb{Z})/n\mathrm{H}_1(X,\mathbb{Z}) = \mathrm{H}_1(X,\mathbb{Z}/n\mathbb{Z}).$$

Le produit d'intersection sur $\mathrm{H}_1(X,\mathbb{Z})$ nous donne alors, pour $n \neq 0$, des couplages parfaits alternés:

$$e_n\colon J[n] \times J[n] \longrightarrow \mathbb{Z}/n\mathbb{Z}.$$

1.2.1 Remark. Ici, nous trouvons des couplages à valeurs dans $\mathbb{Z}/n\mathbb{Z}$, et non dans $\mu_n(\mathbb{C})$. Cela est possible à cause de l'isomorphisme $\mathbb{Z}/n\mathbb{Z} \to \mu_n(\mathbb{C})$, $\overline{a} \mapsto \exp(2\pi ia/n)$. On pourrait "détecter" le fait que c'est en fait à valeurs dans $\mu_n(\mathbb{C})$ si on considérait l'action de $\mathrm{Aut}(\mathbb{C})$ (ici, il faut utiliser que les X aussi sont des variétés algébriques complexes).

1.3 Construction algébrique pour les courbes elliptiques

Soit k un corps (non nécessairement algébriquement clos), et E une courbe elliptique sur k. Donc E est une courbe algebrique sur k, projective, non singulière, de genre un ($\dim_k(\Omega^1(E)) = 1$), et muni d'un point à valeurs dans k que l'on note 0. Une bonne façon abstraite pour voir la loi d'addition sur E est d'utiliser que le morphisme de foncteurs:

$$E \to \mathrm{Pic}^0_{E/k}, \quad (P \in E(S)) \mapsto ([\mathcal{I}_P^\vee \otimes \mathcal{I}_0] \in \mathrm{Pic}^0(E_S)/\mathrm{Pic}(S))$$

est un isomorphisme. Ceci montre à la fois que $\mathrm{Pic}^0_{E/k}$ est représentable, et munit E d'une loi de groupe. Ce point de vu nous permet aussi de comprendre les isogénies duales. En considérant que le cas $S = \mathrm{Spec}(\overline{k})$, avec $k \to \overline{k}$ une clôture algébrique de k, on (re)trouve que $E(\overline{k}) = \mathrm{Div}^0(E_{\overline{k}})/\mathrm{div}(\overline{k}(E)^*)$. (Bien sûr, il faut expliquer les liens entre diviseurs et groupe de Picard.)

1.3.1 Remark. Il est peut-être important de remarquer que l'utilisation du language catégorique en géométrie algébrique est extrèmement utile. Bien que jugée parfois trop difficile, je pense que cela vaut la peine de l'apprendre.

Soit $\phi\colon E \to F$ un morphisme de courbes elliptiques. Alors, pour tout k-schéma S, on a un morphisme de groupes: $\phi^*\colon \mathrm{Pic}(F_S) \to \mathrm{Pic}(E_S)$, qui sont fonctoriels en S, qui induisent donc (Yoneda) un morphisme $\phi^*\colon \mathrm{Pic}^0_{F/k} \to \mathrm{Pic}^0_{E/k}$, et donc un morphisme $\phi^*\colon F \to E$, appelé le dual de ϕ. Une façon de caractériser ϕ^* est: $\phi^*\phi = [\deg(\phi)]$ sur E, et $\phi\phi^* = [\deg(\phi)]$ sur F.

1.3.2 Proposition. *Notation comme ci-dessus, plus l'hypothèse que la caractéristique de k ne divise pas $\deg(\phi)$. Alors la construction suivante donne un couplage parfait:*

$$\ker(\phi)(\overline{k}) \times \ker(\phi^*)(\overline{k}) \longrightarrow \overline{k}^*.$$

Soit Q dans $\ker(\phi^*)(\overline{k})$. Soit $\mathcal{L}$ un $F_{\overline{k}}$-module inversible correspondant à Q. Alors $\phi^*\mathcal{L}$ est isomorphe à $\mathcal{O}_{E_{\overline{k}}}$, et est muni d'une action de $\ker(\phi)(\overline{k})$. On obtient donc une action de $\ker(\phi)(\overline{k})$ sur le $\overline{k}$-espace vectoriel de dimension un $(\phi^*\mathcal{L})(E_{\overline{k}})$, donc un morphisme $\chi_Q\colon \ker(\phi)(\overline{k}) \to \overline{k}^*$. Pour P dans $\ker(\phi)(\overline{k})$ on pose:

$$e_\phi(P, Q) = \chi_Q(P).$$

Si on prend $\phi = [n]$, avec n non multiple de la caractéristique de k, on trouve un accouplement parfait $e_n\colon E(\overline{k})[n] \times E(\overline{k})[n] \to \mu_n(\overline{k})$.

Terminons par quelques remarques. Les e_ϕ et les e_n ont les propriétés usuelles: $e_n(P, P) = 1$ pour tous les P dans $E(\overline{k})[n]$; pour σ dans $\mathrm{Gal}(\overline{k}/k)$, on a: $\sigma(e_\phi(P, Q)) = e_\phi(\sigma(P), \sigma(Q))$. La

théorie donnée dans cette sous-section se généralise directement aux variétés abéliennes quelconques, en notant que $\mathrm{Pic}^0_{A/k}$ est la variété abélienne duale A' de A. On trouve donc des accouplements $e_n\colon A(\overline{k})[n] \times A'(\overline{k})[n] \to \mu_n(\overline{k})$. Le fait que pour une courbe X on trouve des accouplements sur $J(\overline{k})[n]$ résulte du fait que J et J' sont naturellement isomorphes (via la polarisation principale donnée). Je garantis que pour $k = \mathbb{C}$ les deux définitions des e_n sont compatibles, à signe près. On peut bien sûr déterminer ce signe, mais dans ce cas il faut préciser d'abord quelle orientation de $\mathbb{C}$ on utilise (pour l'intersection orientée) et les signes éventuels dans les morphismes tel que $\mathrm{Div}(E) \to \mathrm{Pic}(E)$.

1.4 Construction algébrique pour les courbes quelconques

Soit X une courbe sur un corps algébriquement clos k. Notons J la jacobienne de X: $J = \mathrm{Pic}^0_{X/k}$ (donc $J(k) = \mathrm{Div}^0(X)/\mathrm{div}(k(X)^*)$). Soient $n \neq 0$, P et Q dans $J(\overline{k})[n]$. Soient D et E des représentants dans $\mathrm{Div}^0(X)$ de P et de Q, respectivement, tel que les supports de D et de E sont disjoints. Prenons f et g dans $k(X)^*$ tel que $nD = \mathrm{div}(f)$ et $nE = \mathrm{div}(g)$. Alors on a (encore à un signe près qui ne dépend que du genre de X):

$$e_n(P,Q) = \frac{f(E)}{g(D)} = \frac{\prod_x f(x)^{E_x}}{\prod_x g(x)^{D_x}}.$$

La preuve du fait que ceci ne dépend pas des choix utilise la réciprocité de Weil: $f(\mathrm{div}(g)) = g(\mathrm{div}(f))$, pour f et g dans $k(X)^*$ tel que $\mathrm{div}(g)$ et $\mathrm{div}(f)$ sont disjoints.

1.5 Le point de vue "Ext"

Une façon de vérifier facilement des identités entre des e_ϕ ou entre des e_ϕ et d'autres choses, est de considérer, pour A une variété abélienne, la variété abélienne duale A' comme $\mathbf{Ext}^1(A, \mathbb{G}_\mathrm{m})$. Par exemple, pour $\phi\colon A \to B$ un morphisme surjectif de variétés abéliennes, on applique $\mathbf{Hom}(\cdot, \mathbb{G}_\mathrm{m})$ à la suite exacte courte (de faisceaux pour la topologie fpqc par exemple):

$$0 \to \ker(\phi) \to A \to B \to 0,$$

et on obtient:

$$0 \to \mathbf{Hom}(\ker(\phi), \mathbb{G}_\mathrm{m}) \to \mathbf{Ext}^1(B, \mathbb{G}_\mathrm{m}) \to \mathbf{Ext}^1(A, \mathbb{G}_\mathrm{m}).$$

Ceci donne un isomorphisme entre $\ker(\phi')$ et $\mathbf{Hom}(\ker(\phi), \mathbb{G}_\mathrm{m})$. Soit $\ker(\phi)^0_\mathrm{red}$ le réduit de la composante connexe de 0 de $\ker(\phi)$. Alors $\ker(\phi)^0_\mathrm{red}$ est une variété abélienne, $\ker(\phi)/\ker(\phi)^0_\mathrm{red}$ est un schéma en groupes fini, et $\mathbf{Hom}(\ker(\phi), \mathbb{G}_\mathrm{m}) = (\ker(\phi)/\ker(\phi)^0_\mathrm{red})^D$, le dual de Cartier

de $\ker(\phi)/\ker(\phi)^0_{\mathrm{red}}$. Si $\ker(\phi)$ est fini, on a simplement $\ker(\phi') = \ker(\phi)^D$, ce qui redonne l'accouplement e_ϕ. Un avantage ici est aussi que l'on voit que e_ϕ existe pour $\phi\colon A \to B$ une isogénie entre schémas abéliens, sans hypothèse sur le degré de ϕ.

1.6 Cohomologie étale, de de Rham,...

Pour finir, je tiens à remarquer que l'accouplement de Weil n'est qu'une manifestation de la structure multiplicative sur la cohomologie. En effet, pour $\mathcal{F}$ et $\mathcal{G}$ des faisceaux de groupes abéliens sur un espace topologique X, on a des applications bilinéaires:

$$\mathrm{H}^i(X, \mathcal{F}) \times \mathrm{H}^j(X, \mathcal{G}) \to \mathrm{H}^{i+j}(X, \mathcal{F} \otimes \mathcal{G}).$$

L'accouplement de Weil est directement lié au cup produit sur la cohomologie étale. En effet: pour E une courbe elliptique sur un corps algébriquement clos k on a: $E[n] = \mathrm{H}^1(E_{\mathrm{et}}, \mu_n)$ (en utilisant la suite de Kummer et l'autodualité de E), et $\mathrm{H}^2(E, \mu_n^{\otimes 2}) = \mu_n(k) \otimes \mathrm{H}^2(E, \mu_n) = \mu_n(k)$. De même, il existe un produit sur la cohomologie de de Rham.

Donc, en cas d'urgence, pour des questions sur des accouplements de Weil et choses liées, consultez un "cohomologue".

1.7 Accouplements multilinéaires?

Cette partie a été ajouté après l'exposé, suite à une question de Joux sur la possibilité d'avoir des accouplements multilinéaires, ce qui serait intéressant pour des secrets communs entre groupes de personnes. J'ai dit:

> Comme l'accouplement de Weil peut être vu comme le produit entre $\mathrm{H}^1(E_{\overline{k},\mathrm{et}}, \mu_n)$ et lui même à valeurs dans $\mathrm{H}^2(E_{\overline{k},\mathrm{et}}, \mu_n^{\otimes 2}) = \mu_n(k)$, on pourra peut-être généraliser cela en regardant des produits avec plus de facteurs, par exemple:
>
> $$\mathrm{H}^1 \times \mathrm{H}^1 \times \mathrm{H}^1 \times \mathrm{H}^1 \to \mathrm{H}^4,$$
>
> sur une surface.

Maintenant (trois jours plus tard), j'ai réfléchi un peu, et je ne suis pas optimiste. Pour la surface on pourrait prendre un produit de deux fois la même courbe elliptique, $E \times E$, par exemple. Dans ce cas on a (formule de Künneth):

$$\mathrm{H}^1(E^2_{\overline{k}}, \mu_n) = \mathrm{H}^1(E_{\overline{k}}, \mu_n) \oplus \mathrm{H}^1(E_{\overline{k}}, \mu_n) = E(\overline{k})[n] \oplus E(\overline{k})[n].$$

Le produit donne:

$$\mathrm{H}^1(E^2_{\overline{k}}, \mu_n)^4 \longrightarrow \mathrm{H}^4(E^2_{\overline{k}}, \mu_n^{\otimes 4}) = \mu_n(\overline{k})^{\otimes 2} \otimes \mathrm{H}^4(E^2_{\overline{k}}, \mu_n^{\otimes 2}) = \mu_n(\overline{k})^{\otimes 2}.$$

Tout le problème est dans le groupe $\mu_n(\overline{k})^{\otimes 2}$. Les calculs des produits ne posent pas de problème, mais on trouvera les résulats sous la forme (quand on écrit additivement le groupe $\mu_n(\overline{k})$) de somme finie $\sum_i x_i \otimes y_i$. Le problème est de décider quand deux sommes comme ça définissent le même élément! Ce problème semble difficile si on veut supposer le log discrèt dans le groupe $\mu_n(\overline{k})$ soit difficile.

Une leçon à ne pas oublier de ceci est: même un groupe qui paraît bien facile pour le calcul tel que $\mu_n(\overline{k})^{\otimes 2}$ peut être non utilisable, car on ne voit pas comment décider l'égalité des éléments donnés sous la forme de sommes finies de termes $x \otimes y$. N'oublions pas que tout le problème du log discrèt sur $\mu_n(\overline{k})$ est qu'on n'a pas de générateur de $\mathrm{Hom}(\mu_n(\overline{k}), \mathbb{Z}/n\mathbb{Z})$, donc pas d'élément utile de $\mu_n(\overline{k})^{\otimes -1}$!

1.8 Pourquoi accoupler un point avec lui-même peut être utile

Bien sûr, on a un peu peur quand on voit $e(P, P)$, car on a tendance à croire que les accouplements e sont alternés, donc que $e(P, P) = 1$. Mais pour e associé à une isogénie qui n'est pas forcément de la forme multiplication par un entier, cela peut donner des choses utiles.

Soit p un nombre premier, E une courbe elliptique sur $\mathbb{F}_p$. Alors $E(\mathbb{F}_p) = \ker(F - 1)$, où $F\colon E \to E$ est l'endomorphisme de Frobenius de E. Notons V la duale de F. On a donc un accouplement parfait:

$$e_{F-1}\colon \ker(F-1) \times \ker(V-1) \longrightarrow \overline{\mathbb{F}}_p^*.$$

Maintenant, on se pose la question si par hasard il peut arriver que $F - 1$ et $V - 1$ ont le même noyau. Une façon d'avoir ça est d'avoir $F = V$, mais sur $\mathbb{F}_p$ cela n'est pas possible (c'est bien possible sur $\mathbb{F}_{p^2}$, avec $F = V = -p$, par exemple). Mais une autre façon est d'avoir $F - 1 = 1 - V$, ce qui correspond exactement à la condition $|E(\mathbb{F}_p)| = p - 1$.

Donc, pour résumer: si $E(\mathbb{F}_p)$ est de cardinal $p - 1$, alors e_{F-1} est un accouplement parfait (et symétrique, sans doute) sur $E(\mathbb{F}_p)$ et lui-même.