This is Chapter 7 by Gerhard Frey and Tanja Lange of the Handbook of Elliptic and Hyperelliptic Curve Cryptography, Henri Cohen, Christophe Doche, and Gerhard Frey, Editors, CRC Press 2006.

Chapter 7

Background on Weil Descent

Gerhard Frey and Tanja Lange

Contents in Brief

Weil descent — or, as it is alternatively called — *scalar restriction*, is a well-known technique in algebraic geometry. It is applicable to all geometric objects like curves, differentials, and Picard groups, if we work over a separable field L of degree d of a ground field K.

It relates t-dimensional objects over L to td-dimensional objects over K. As guideline the reader should use the theory of algebraic curves over $\mathbb{C}$, which become surfaces over $\mathbb{R}$. This example, detailed in Section 5.1.2, already shows that the structure of the objects after scalar restriction can be much richer: the surfaces we get from algebraic curves carry the structure of a Riemann surface and so methods from topology and Kähler manifolds can be applied to questions about curves over $\mathbb{C}$.

This was the reason to suggest that Weil descent should be studied with respect to (constructive and destructive) applications for DL systems [FRE 1998]. We shall come to such applications in Sections 15.3 and 22.3.

In the next two sections we give a short sketch of the mathematical properties of Weil descent. The purpose is to provide a mathematical basis for the descent and show how to construct it. For a thorough discussion in the frame of algebraic geometry and using the language of schemes, we refer to [DIE 2001].

7.1 Affine Weil descent

We begin with the easiest case. Let V be an affine variety in the affine space $\mathbb{A}_L^n$ over L defined by m equations

$$F_i(x_1, \ldots, x_n) = 0;\ i = 1, \ldots, m$$

with $F_i(x) \in L[x_1, \ldots, x_n]$.

We want to find an affine variety $W_{L/K}(V)$ defined over K with the following properties:

(W1) For any field $K' \subset \overline{K}$ for which the degree of $L \cdot K'$ over K' is equal to d (i.e., K' is linearly disjoint from L over K) we have a natural identification of $W_{L/K}(V)(K')$ with $V(L \cdot K')$.

(W2) The variety $W_{L/K}(V)_L$ obtained from $W_{L/K}(V)$ by base extension from K to L is isomorphic to V^d, the d-fold Cartesian product of V with itself.

To achieve this we choose a basis $\{u_1, \ldots, u_d\}$ of L as K-vector space. Then we define the nd variables $y_{i,j}$ by

$$x_i = u_1 y_{1,i} + \cdots + u_d y_{d,i}, \quad \text{for } i = 1, \ldots, n.$$

We replace the variables x_i in the relations defining V by these expressions.

Next we write the coefficients of the resulting relations as K-linear combinations of the basis $\{u_1, \ldots, u_d\}$ and order these relations according to this basis. As result we get m equations of the form

$$G_i(y) = g_{i,1}(y)u_1 + \cdots + g_{i,d}(y)u_d = 0$$

with $g_{i,j} \in K[y_{1,1}, \ldots, y_{n,d}]$. Because of the linear independence of the elements u_i and because of condition W1 we see that we have to define W as the Zariski closed subset in $\mathbb{A}^{nd}$ given by the md equations

$$g_{i,j}(y) = 0.$$

Proposition 7.1 Let V and W be as above. Then W is an affine variety defined over K satisfying the conditions W1 and W2. So W is the Weil descent $W_{L/K}(V)$ of V.

Example 7.2 Let V be equal to the affine space of dimension n over L with coordinate functions $x_1, \ldots, x_n$.

Then $W_{L/K}(V) = \mathbb{A}^{nd}$ with coordinate functions $y_{i,j}$ defined by

$$x_i = u_1 y_{1,i} + \cdots + u_d y_{d,i}.$$

As a special case, take $L = \mathbb{C}$ and $K = \mathbb{R}$, $n = 1$, and take as complex coordinate function the variable z and as basis of $\mathbb{C}/\mathbb{R}$, the elements $1, i$ with $i^2 = -1$.

As usual we choose real variables x, y satisfying the identity

$$z = x + iy.$$

A polynomial or more generally a rational function $G(z)$ in z gives rise to a function in $G_{\mathbb{R}}(x, y)$ that we can interpret as a function from $\mathbb{R}^2$ to $\mathbb{C}$. We separate its real and imaginary part and get

$$G(z) = g_1(x, y) + ig_2(x, y).$$

Example 7.3 Assume that $L = K(\alpha)$ with $\{1, \alpha, \alpha^2\}$ a basis of L/K and $\alpha^3 = b \in K$ and assume that $\mathrm{char}(K) \neq 3$.

Take the affine part of the elliptic curve given by the equation

$$E_a : x_1^2 - x_2^3 - 1 = 0.$$

Replace x_i by $y_{1,i} + \alpha y_{2,i} + \alpha^2 y_{3,i}$ to get the equation

$$\left(y_{1,1} + \alpha y_{2,1} + \alpha^2 y_{3,1}\right)^2 - \left(y_{1,2} + \alpha y_{2,2} + \alpha^2 y_{3,2}\right)^3 - 1 = 0.$$

This yields the following system of equations

$$\begin{aligned} y_{1,1}^2 + 2by_{2,1}y_{3,1} - y_{2,1}^3 - b^2y_{3,2}^3 - by_{2,3}^3 - 6by_{1,2}y_{2,2}y_{3,2} - 1 &= 0 \\ by_{1,3}^2 + 2y_{1,1}y_{2,1} - 3y_{1,2}^2y_{2,2} - 3by_{2,2}^2y_{3,2} - 3by_{1,2}y_{3,2}^2 &= 0 \\ y_{1,2}^2 + 2y_{1,1}y_{3,1} - 3y_{1,2}^2y_{3,2} - 3y_{1,2}y_{2,2}^2 - 3by_{2,2}y_{3,2}^2 &= 0 \end{aligned}$$

which defines the Weil descent $W_{L/K}(E_a)$ of E_a.

Remark 7.4 The example is interesting since it is an open affine part of an abelian variety of dimension 3 defined over K, whose rational points are in a natural way equal to the L-rational points of the elliptic curve E.

7.2 The projective Weil descent

Having defined the Weil descent for affine varieties we proceed in the usual way to define it for projective varieties V defined over L, which are embedded in some projective space $\mathbb{P}_L^n$.

We cover V by affine subvarieties V_i and apply the restriction of scalars to the V_i to get a collection of affine varieties $W_{L/K}(V_i) =: W_i$ over K. The varieties V_i are intersecting in Zariski open parts of V and there are rational maps from V_i to V_j induced by the rational maps between the different embeddings of the affine space $\mathbb{A}_L^n$ into $\mathbb{P}_L^n$ (cf. Example 4.44). By using the functoriality properties of the Weil descent (or by a direct computation in the respective coordinates as in the examples) one concludes that the affine varieties W_i can be glued together in a projective space (which is the Weil descent of $\mathbb{P}_L^n$). If we take the coverings fine enough we get as a result of the gluing process a projective variety $W_{L/K}(V)$.

Warning. Not every cover of V by affine subvarieties V_i has the property that the varieties $W_{L/K}(V_i)$ cover $W_{L/K}(V)$. For instance let E be a plane projective elliptic curve given by the equation

$$E : Y^2Z = X^3 + a_4XZ^2 + a_6Z^3.$$

Then E is covered by the affine curves E_1 and E_2 one gets by intersecting $\mathbb{P}_L^2$ with the open parts for which $Z \neq 0$ (respectively $Y \neq 0$) holds. But we also need E_3, which is the intersection of E with the open part of $\mathbb{P}^2$ defined by $X \neq 0$ to get $W_{L/K}(E)$ by the gluing procedure described above.

There is another complication if we want to describe the projective variety $W_{L/K}(V)$ explicitly as a subvariety of the projective space $\mathbb{P}^N$: the dimension of this space can become rather large. Here is an estimate for this dimension:

Lemma 7.5 Let V be a projective variety embedded into $\mathbb{P}_L^n$. Then $W_{L/K}(V)$ can be embedded (in a canonical way) into $\mathbb{P}^{(n+1)^d-1}$.

This lemma follows from the construction via affine covers and the application of the Segre map (cf. Examples 4.13 and 4.25) of products of projective spaces into a projective space.

We can summarize our results and get the following theorem:

Theorem 7.6 Let L/K be a finite separable field extension of degree d. Let V be an affine or a projective variety defined over L. The Weil restriction $W_{L/K}(V)$ satisfies the properties W1 and W2. If V is affine (respectively projective) and has dimension t then $W_{L/K}(V)$ is an affine (respectively projective) variety defined over K of dimension td.

Again by functoriality properties one can conclude that the Weil restriction of an algebraic group is again an algebraic group. Hence we get:

Corollary 7.7 The Weil restriction of an abelian variety $\mathcal{A}$ over L is an abelian variety $W_{L/K}(\mathcal{A})$ over K.

Let $\mathcal{A}_1$ be a Zariski-open nonempty affine subvariety of $\mathcal{A}$. Then $W_{L/K}(\mathcal{A}_1)$ is an affine Zariski-open nonempty subvariety of $W_{L/K}(\mathcal{A})$ and hence it is birationally equivalent to $W_{L/K}(\mathcal{A})$.

This corollary justifies Remark 7.4.

7.3 Descent by Galois theory

In the last sections we have introduced an explicit method to construct the Weil descent of varieties by using affine coordinates. The advantage of this approach is the explicit definition of the Weil descent by equations. The disadvantage is that the number of variables and the number of relations grow and so the description becomes very complicated. This is especially striking if we want to apply the descent to projective varieties or if the degree of L/K is not small. For many purposes it is enough to have the Weil descent and its properties as background. Then we apply it using definitions by Galois theory as this is much more elegant.

This approach becomes most natural if we assume that L/K *is a Galois extension with relative Galois group* $G(L/K) = G$. Note that for us the most important case is that K and L are finite fields and then this assumption is always satisfied.

Let V be a variety defined over L and let $\sigma \in G$ be an automorphism of L fixing K.

We want to define the image of V under σ. We assume that V is affine. If V is projective one can proceed in a completely analogous way.

We choose affine coordinate functions $x = (x_1, \ldots, x_n)$ of $\mathbb{A}^n_L$ and define the points on V as the set of zeroes of the equations defining V as usual. Let I be the prime ideal generated by these equations in $L[x]$. We apply σ to the coefficients of rational functions F in $L(x)$ and denote by $\sigma \cdot F$ the image.

The ideal $I_\sigma := \sigma \cdot I$ is again a prime ideal in $L[x]$ and so it defines an affine variety V^σ over L. Let us extend σ to an automorphism $\tilde{\sigma}$ of $\overline{K}$. By definition we get $\tilde{\sigma} \cdot I = \sigma \cdot I$ and so $V^{\tilde{\sigma}} = V^\sigma$ does not depend on the choice of the extension. Let P be a point in $V(\overline{K})$. Then $\tilde{\sigma}(P)$ is a point in $V^\sigma(\overline{K})$ and conversely. So $V^\sigma(\overline{K}) = \tilde{\sigma} \cdot V(\overline{K})$.

For all points $Q \in V^\sigma(\overline{K})$ and $f \in L(V)$ we get the identity

$$(\sigma \cdot f)(Q) = \tilde{\sigma}\big(f\big(\tilde{\sigma}^{-1}(Q)\big)\big).$$

In particular, it follows that we can interpret $\sigma \cdot f$ as rational function on V^σ.

We apply this to the functions x_i. To clarify what we mean, we denote by $x_{i,\sigma}$ the function on V^σ induced by the coordinate function x_i, i.e., $x_{i,\sigma}$ is the image of x_i in $L[x]/(\sigma \cdot I)$. We get: let P be a point in V and let $x_i(P)$ be the value of the i-th coordinate function on V applied to P. Let $x_{i,\sigma}$ be the i-th coordinate function on V^σ. Then $x_{i,\sigma} = \sigma \cdot x_i$ and the value of $x_{i,\sigma}$ applied to $\tilde{\sigma}(P)$ is equal to $\tilde{\sigma}(x_i(P))$.

All these considerations are near to tautological statements but they allow us to define an action of the absolute Galois group G_K of K on the variety

$$W := \prod_{\sigma \in G} V^\sigma.$$

Indeed let $P := (\ldots, P_\sigma, \ldots)_{\sigma \in G}$, with $P_\sigma \in V^\sigma(\overline{K})$, be a point in $W(\overline{K})$. Let $\tilde{\tau}$ be an element of G_K whose restriction to L is equal to τ. Then

$$\tilde{\tau}(P) := (\ldots, Q_\sigma, \ldots)_{\sigma \in G} \text{ with } Q_\sigma = \tilde{\tau}(P_{\tau^{-1} \circ \sigma}).$$

Theorem 7.8 The variety W is equal to the Weil restriction $W_{L/K}(V)$.

Proof. To prove this theorem we check the properties characterizing the Weil descent.

First W is a variety defined over L. As we have seen its set of points is invariant under the action of G_K. So W is a variety defined over K.

A point $P \in W$ is K-rational if and only if it is L-rational and for all $\tau \in G$ we have

$$\tau(P_{\tau^{-1}\circ\sigma}) = P_\sigma.$$

Taking $\tau = \sigma^{-1}$ this means that $P_\sigma = \sigma^{-1}P_{\mathrm{Id}}$ for all $\sigma \in G$ with $P \in V(L)$. It follows that $W(K) = V(L)$.

Next we extend the ground field K to L and look at W_L. On the Galois theoretic side this means that we restrict the Galois action of G_K on W to an action of G_L. But this group leaves each V^σ invariant and so W_L is isomorphic to $\prod_{\sigma\in G} V = V^d$. □

We shall be interested in the special case that $K = \mathbb{F}_q$ and $L = \mathbb{F}_{q^d}$.

Corollary 7.9 Let V be a (projective or affine) variety defined over $\mathbb{F}_{q^d}$ of dimension t. For $i = 0, \ldots, d-1$ let V_i be the image of V with respect to ϕ_q^i (cf. Proposition 5.67).

Then

$$W(V) := \prod_{i=0}^{d-1} V_i$$

is a variety defined over $\mathbb{F}_q$ of dimension td which is K-isomorphic to $W_{\mathbb{F}_{q^d}/\mathbb{F}_q}(V)$.

If V is affine (respectively projective) then $W(V)$ is an affine (respectively projective) variety defined over K.

If V is an abelian variety over $\mathbb{F}_{q^d}$ then $W(V)$ is an abelian variety over $\mathbb{F}_q$.

The action of ϕ on $W(V)$ is given as follows: Let $P = (\ldots, P_i, \ldots)$ be a point in $W(V)(\overline{K})$. Then $\phi_q(P) = (\ldots, Q_i, \ldots)$ with $Q_i = \phi_q(P)_{(i-1 \bmod d)}$.

Remark 7.10 In general the Weil restriction of a Jacobian variety is not a Jacobian variety.

7.4 Zariski closed subsets inside of the Weil descent

As mentioned already, one main application of the Weil descent method is that in $W_{L/K}$ there are Zariski closed subsets which cannot be defined in V.

In the following we shall describe strategies to find such subsets.

7.4.1 Hyperplane sections

To simplify the discussion we assume that V is affine with coordinate functions $x_1, \ldots, x_n$ and we take the description of $W_{L/K}(V)$ given in Proposition 7.1. There we have introduced nd coordinates functions $y_{i,j}$ for $W_{L/K}(V)$ by

$$x_i = u_1 y_{1,i} + \cdots + u_d y_{d,i}, \quad \text{for } i = 1, \ldots, n,$$

where $\{u_1, \ldots, u_d\}$ is a basis of L/K. Take $J \subset \{1, \ldots, d\} \times \{1, \ldots, n\}$ and adjoin the equations $y_{i,j} = 0$ for $(i,j) \in J$ to the equations defining $W_{L/K}(V)$.

The resulting Zariski closed set inside of $W_{L/K}(V)$ is denoted by W_J. It is the intersection of the Weil restriction of V with the affine hyperplanes defined by $y_{i,j} = 0$; $(i,j) \in J$.

"In general" we can expect that W_J is again a variety over K of dimension $td - |J|$.

Example 7.11 Let E be an elliptic curve defined over L given by a Weierstraß equation

$$E : x_1^2 + a_1 x_1 x_2 + a_3 x_1 = f(x_2),$$

where f is monic of degree 3. Take $1 \leqslant m \leqslant d-1$ and $J = \{1, \ldots, m\} \times \{2\}$.

Then $W_J(K)$ consists of all points in $E(L)$ whose x_2-coordinate is a K-linear combination of the elements $u_1, \ldots, u_m$.

Remark 7.12 This example is the mathematical background of a subexponential attack to the discrete logarithm in elliptic curves over nonprime fields found recently by Gaudry and Diem (cf. Section 22.3.5).

7.4.2 Trace zero varieties

We assume for simplicity that $L = \mathbb{F}_{q^d}$ and $K = \mathbb{F}_q$ and we use the Galois theoretic description of the Weil descent.

Let V be a variety defined over K. So we get $V^{\phi_q} = V$. Note that nevertheless $W_{\mathbb{F}_{q^d}/\mathbb{F}_q}(V)$ is *not* $\mathbb{F}_q$-isomorphic to V^d because of the twisted Galois operation. But we can embed V into $W_{\mathbb{F}_{q^d}/\mathbb{F}_q}(V)$ as diagonal:

Map the point $P \in V(\overline{K})$ to the point $(\ldots, \phi_q^i(P), \ldots) \in \prod_{i=0}^{d-1} V$. By this map we can identify V with a subvariety of $W_{\mathbb{F}_{q^d}/\mathbb{F}_q}(V)$.

Now assume in addition that $V = \mathcal{A}$ is an abelian variety. Then we find a complementary abelian subvariety to $\mathcal{A}$ inside of $W_{\mathbb{F}_{q^d}/\mathbb{F}_q}(\mathcal{A})$.

We use the existence of an automorphism π of order d of $W_{\mathbb{F}_{q^d}/\mathbb{F}_q}(\mathcal{A})$ defined by

$$P = (\ldots, P_i, \ldots) \mapsto \pi(P) = (\ldots, Q_i, \ldots) \text{ with } Q_i = P_{i-1 \bmod d}.$$

The map π is obviously an automorphism over $\mathbb{F}_{q^d}$. To prove that π is defined over $\mathbb{F}_q$ we have to show that π commutes with the action of ϕ_q. But

$$\pi(\phi_q(P)) = (\ldots, Q_i', \ldots) \text{ with } Q_i' = \phi_q(Q_{i-2 \bmod d})$$

and this is equal to $\phi_q\big(\pi(P)\big)$.

Denote by $\mathcal{A}_0$ the kernel of the endomorphism $\sum_{i=0}^{d-1} \pi^i$. It is an abelian subvariety of $\mathcal{A}$ and it is called the *trace zero subvariety* of $\mathcal{A}$. Note that the intersection set of $\mathcal{A}$ — embedded as diagonal into $W_{\mathbb{F}_{q^d}/\mathbb{F}_q}(\mathcal{A})$ — with $\mathcal{A}_0$ consists of the points of $\mathcal{A}$ of order dividing d, and the $\mathbb{F}_q$-rational points of $\mathcal{A}_0$ are the points P in $\mathcal{A}(\mathbb{F}_{q^d})$ with $\mathrm{Tr}(\phi_q)(P) = 0$.

To see that $\mathcal{A}$ and $\mathcal{A}_0$ generate $W_{\mathbb{F}_{q^d}/\mathbb{F}_q}(\mathcal{A})$ we use that $\mathcal{A}$ is the kernel of $\pi - \mathrm{Id}$ and that $\mathcal{A}_0$ contains $(\pi - \mathrm{Id})\big(W_{\mathbb{F}_{q^d}/\mathbb{F}_q}(\mathcal{A})\big)$.

We summarize:

Proposition 7.13 Let $\mathcal{A}$ be an abelian variety defined over $\mathbb{F}_q$. We use the product representation of $W_{\mathbb{F}_{q^d}/\mathbb{F}_q}(\mathcal{A})$ and define π as automorphism induced by a cyclic permutation of the factors. Then we have the following results:

1. $\mathcal{A}$ can be embedded (as diagonal) into $W_{\mathbb{F}_{q^d}/\mathbb{F}_q}(\mathcal{A})$. Its image under this embedding is the kernel of $\pi - \mathrm{Id}$.
2. The image of $\pi - \mathrm{Id}$ is the trace zero subvariety $\mathcal{A}_0$.
3. The $\mathbb{F}_q$-rational points of $\mathcal{A}_0$ are the images of points $P \in \mathcal{A}(\mathbb{F}_{q^d})$ with $\mathrm{Tr}(\pi)(P) = 0$.
4. Inside of $W_{\mathbb{F}_{q^d}/\mathbb{F}_q}(\mathcal{A})$ the subvarieties $\mathcal{A}$ and $\mathcal{A}_0$ intersect in the group of points of $\mathcal{A}$ of order dividing d.

For an example with $\mathcal{A} = E$ an elliptic curve and $d = 3$ we refer to [FRE 2001]; for $\mathcal{A} = J_C$ being the Jacobian of a hyperelliptic curve C, see [LAN 2004c]. We further investigate these constructive applications of Weil descent in Section 15.3.

7.4.3 Covers of curves

Let C be a curve defined over $\mathbb{F}_{q^d}$ with Jacobian variety J_C. We want to apply Weil descent to get information about Pic^0_C from $W_{\mathbb{F}_{q^d}/\mathbb{F}_q}(J_C)(\mathbb{F}_q)$.

Here we investigate the idea of looking for curves C' defined over $\mathbb{F}_q$ that are embedded into $W_{\mathbb{F}_{q^d}/\mathbb{F}_q}(J_C)$. Then the Jacobian of C' has $W_{\mathbb{F}_{q^d}/\mathbb{F}_q}(J_C)$ as a factor and we can use information about $\mathrm{Pic}^0_{C'}$ to study Pic^0_C. Of course this is only a promising approach if the genus of C' is not too large.

One can try to construct C' directly, for instance, by using hyperplane sections. But it is very improbable that this will work if we are not in very special situations. Hence, it is not clear whether this variant can be used in practice. But this approach leads to interesting mathematical questions:

- Which abelian varieties have curves of small genus as sub-schemes?
- Which curves can be embedded into Jacobian varieties of modular curves?
- Which curves have the scalar restriction of an abelian variety (e.g., an elliptic curve) as Jacobian?

In [BODI$^+$ 2004] one finds families of curves for which the last question is answered positively.

7.4.4 The GHS approach

In practice another approach is surprisingly successful. *A priori* it has nothing to do with Weil descent, but as a background and in order to prove results the Weil descent method is useful.

Let L be a Galois extension of the field K. In our applications we shall take $L = \mathbb{F}_{q^d}$ and $K = \mathbb{F}_q$. Assume that C is a projective irreducible nonsingular curve *defined over* L, and D is a projective irreducible nonsingular curve *defined over* K.

Let

$$\varphi : D_L \to C$$

be a nonconstant morphism defined over L. As usual we denote by φ^* the induced map from Pic^0_C to $\mathrm{Pic}^0_{D_L}$. It corresponds to the conorm map of divisors in the function fields $\varphi^*\big(L(C)\big) \subset L(D_L)$. Next we use the inclusion $K(D) \subset L(D_L)$ to define a correspondence map on divisor classes

$$\psi : \mathrm{Pic}^0(C) \to \mathrm{Pic}^0(D)$$

given by

$$\psi := \mathrm{N}_{L/K} \circ \varphi^*,$$

where $\mathrm{N}_{L/K}$ is the norm of L/K.

Assume that we are interested in a subgroup G (for instance, of large prime order ℓ) in Pic^0_C and assume that we can prove that $G \bigcap \ker(\psi) = \{0\}$. Then we have transferred the study of G as subgroup of a Jacobian variety over L to the study of a subgroup of a Jacobian variety over K which may be easier.

The relation with the Weil descent method is that by the Weil descent of the cover map φ we get an embedding of D into $W_{L/K}(J_C)$. This method is the background of the so-called GHS algorithm. We shall come to this in more detail in 22.3.2.

The mathematically interesting aspect of this method is that it relates the study of Picard groups of curves to the highly interesting theory of fundamental groups of curves over non-algebraically closed ground fields.