Lecture 11

January 13, 2005
Notes by Ivo Dell'Ambrogio

§24 Pairings and Cartier duality

Logically, this section could have followed right after §4. Let G, G' and H be commutative group schemes over a scheme S.

Definition. A morphism $G' \times_S G \to H$ of schemes over S is called *bilinear* if it is additive in each factor, or equivalently, if for every scheme T over S the induced map $G'(T) \times G(T) \to H(T)$ is bilinear in the usual sense. The group of such bilinear morphisms will be denoted by $\mathrm{Bilin}_S(G' \times_S G, H)$.

Definition. Denote by $\underline{\mathrm{Hom}}_S(G, H)$ the contravariant functor

$$\mathfrak{Sch}_S \to \mathfrak{Ab},\ T \mapsto \underline{\mathrm{Hom}}_S(G, H)(T) := \mathrm{Hom}_T(G_T, H_T).$$

If it is representable, the representing group scheme over S will also be denoted by $\underline{\mathrm{Hom}}_S(G, H)$.

Note. One can show that $\underline{\mathrm{Hom}}_S(G, H)$ is representable whenever G is finite and flat over S. Unfortunately, the detailed study of $\mathrm{Bilin}_S(G' \times_S G, H)$ and $\underline{\mathrm{Hom}}_S(G, H)$ is beyond the scope of this course because of time constraints.

Proposition 24.1 (Adjunction formula). There exists an isomorphism

$$\mathrm{Bilin}_S(G' \times_S G, H) \cong \mathrm{Hom}_S(G', \underline{\mathrm{Hom}}_S(G, H)),$$

which is functorial in all variables. This of course determines $\underline{\mathrm{Hom}}_S(G, H)$ up to natural isomorphism.

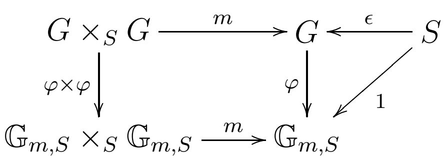
Proof. By definition giving a morphism $\varphi\colon G' \to \underline{\mathrm{Hom}}_S(G, H)$ is equivalent to giving a homomorphism $\varphi'\colon G' \times_S G \longrightarrow G' \times_S H$ of group schemes over G'. Thus φ' must be a morphism of schemes over S whose first component is the projection to G' and whose second component is a morphism $\psi\colon G' \times_S G \to H$ that is additive in G. Moreover, one easily checks that φ is additive if and only if ψ is additive in G'. This sets up the desired bijection, and one easily checks that it is a group isomorphism and functorial in all variables. $\square$

Definition. A bilinear morphism $\beta : G' \times_S G \to H$ is *nondegenerate at G'* if, for all $T \to S$ and all $0 \neq g' \in G'(T)$, the homomorphism $\beta(g', -) : G_T \to H_T$ is nontrivial. One similarly defines the notion *nondegenerate at G*.

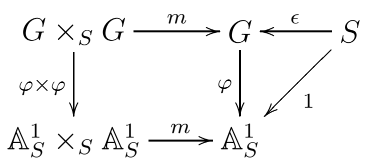
Note. It is clear that β is nondegenerate at G' if and only if the associated homomorphism $G' \to \underline{\mathrm{Hom}}_S(G, H)$ is a monomorphism.

Proposition 24.2. If G is finite flat over S, there is a functorial isomorphism $\underline{\mathrm{Hom}}_S(G, \mathbb{G}_{m,S}) \cong G^*$, and in particular $\underline{\mathrm{Hom}}_S(G, \mathbb{G}_{m,S})$ is representable.

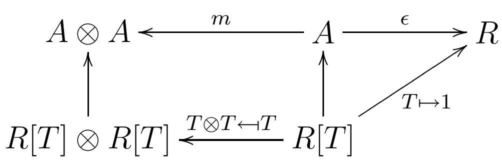
Proof. For all schemes T over S we must construct a natural isomorphism $\mathrm{Hom}_T(G_T, \mathbb{G}_{m,T}) \cong G^*(T)$. By passing to an affine covering of T it suffices to do this when T itself is affine. After replacing $G \to S$ by $G_T \to T$, we may also assume that $T = S$. As usual, we then write $S = \operatorname{Spec} R$, $G = \operatorname{Spec} A$, and $G^* = \operatorname{Spec} A^*$, where $A^* = \mathrm{Hom}_R(A, R)$. By definition, $\mathrm{Hom}_S(G, \mathbb{G}_{m,S})$ is the group of morphisms $\varphi\colon G \to \mathbb{G}_{m,S}$ of schemes over S such that the left hand side of the following diagram commutes:



Since every homomorphism maps the unit element to the unit element, the whole diagram then commutes. Next, these morphisms are in bijection to morphisms $\varphi : G \to \mathbb{A}^1_S$ of schemes over S such that



commutes; in fact, every such $\varphi : G \to \mathbb{A}^1_S$ automatically lands inside $\mathbb{G}_{m,S}$, because for every point g of G we have $\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(\epsilon) = 1$, showing that $\varphi(g)$ is invertible. These morphisms in turn correspond to R-algebra homomorphisms $R[T] \to A$ such that



commutes. But giving an R-algebra homomorphism $R[T] \to A$ is equivalent to giving the image a of T, so we obtain a bijection to the set

$$\big\{a \in A \;\big|\; m(a) = a \otimes a,\ \epsilon(a) = 1\big\}.$$

By biduality $A \cong A^{**}$ we can identify this with the set

$$\big\{\alpha \in \operatorname{Hom}_R(A^*, R) \;\big|\; \forall \ell, \ell' \in A^*\colon\; \alpha(m^*(\ell\otimes\ell')) = \alpha(\ell)\cdot\alpha(\ell'),\; \alpha(\epsilon^*(1)) = 1\big\}.$$

Finally, these conditions say precisely that $\alpha\colon A^* \to R$ is a homomorphism of R-algebras, i.e., corresponding to a point in $G^*(S)$. The additivity and functoriality are left to the reader. □

Proposition 24.3. If G' and G are both finite flat over S, then a bilinear morphism $\beta : G' \times_S G \to \mathbb{G}_{m,S}$ is nondegenerate at G' and G if and only if its adjoint $G' \to \underline{\operatorname{Hom}}_S(G, \mathbb{G}_{m,S}) = G^*$ is an isomorphism.

Proof. We have seen that β is nondegenerate at G' if and only if its adjoint $\varphi : G' \to G^*$ is a monomorphism. Similarly, β is nondegenerate at G if and only if its adjoint (after having swapped G' and G!) $\varphi' : G \to G'^*$ is a monomorphism. After the conscientious reader has checked that $\varphi' = \varphi^*$, she will see that the second fact is equivalent to φ being an epimorphism. □

§25 Cartier duality of finite Witt group schemes

From this section onwards we will again work over a perfect field k of characteristic $p > 0$. Our aim is to construct natural isomorphisms $(W_m^n)^* \cong W_n^m$ for all m and n and to describe their relation with the action of E and with all transition maps. The existence of an isomorphism $(W_m^n)^* \cong W_n^m$ alone can be proved without the following technicalities, merely by characterizing W_n^m up to isomorphism by a few simple properties. This makes a nice exercise for the interested reader.

By Proposition 24.3 it suffices to construct a nondegenerate pairing $W_n^m \times W_m^n \to \mathbb{G}_{m,k}$, and for this we use the multiplication of Witt vectors. Recall our notation $W_n = W/V^nW$ and $W_n^m = \ker(F^m|W_n)$. For all n and m consider the morphisms

$$\tau_n^m : W_n^m \to W,\; (x_0, \ldots, x_{n-1}) \mapsto (x_0, \ldots, x_{n-1}, 0, 0, \ldots).$$

Their images form a system of infinitesimal neighborhoods of 0 inside W, and we are interested in the formal scheme $\widehat{W} := \bigcup_{n,m} \tau_n^m(W_n^m)$. Its points over any k-algebra R are the elements $\underline{x} \in W(R)$ such that all components x_i are nilpotent and almost all are zero.

Lemma 25.1. (a) Addition in W induces a morphism $\widehat{W} \times \widehat{W} \to \widehat{W}$.
(b) Multiplication in W induces a morphism $W \times \widehat{W} \to \widehat{W}$.
In other words, $\widehat{W}(R)$ is an ideal in $W(R)$ for all R.

Proof. The phantom component $\Phi_n(\underline{x}) = x_0^{p^n} + px_1^{p^{n-1}} + \cdots + p^n x_n$ is an isobaric polynomial of degree p^n, if we set $\deg(x_i) = p^i$. Recall that addition in W is given by $\underline{x} + \underline{y} = \underline{s} = (s_0, s_1, \ldots)$, where the s_i are polynomials in $\mathbb{Z}[\underline{x}, \underline{y}]$ characterized by $\Phi_n(\underline{s}) = \Phi_n(\underline{x}) + \Phi_n(\underline{y})$, this last being the usual addition. Thus $\Phi_n(\underline{s})$ is isobaric of degree p^n when $\deg(x_i) = \deg(y_i) = p^i$, which in turn implies by induction that s_n is isobaric of degree p^n. Plugging in any $\underline{x}$, $\underline{y} \in \widehat{W}(R)$, we deduce that $s_i(\underline{x}, \underline{y})$ is nilpotent for all i and that it is zero for $i \gg 0$. This proves (a).

For (b) we similarly note that multiplication in W is given by $\underline{x} \cdot \underline{y} = \underline{p} = (p_0, p_1, \ldots)$, where $\Phi_n(\underline{p}) = \Phi_n(\underline{x}) \cdot \Phi_n(\underline{y})$. One finds that $p_n \in \mathbb{Z}[\underline{x}, \underline{y}]$ is isobaric of degree p^n when $\deg(y_i) = p^i$ and $\deg(x_i) = 0$, and then one concludes with the same argument. □

Note. Lemma 25.1 (a) defines an additive group structure on the formal scheme $\widehat{W}$, making it a "group formal scheme", that is, a group object in the category of formal schemes. However, the morphisms $\tau_n^m\colon W_n^m \to \widehat{W}$ are no group homomorphisms and their images no group subschemes, so $\widehat{W}$ should not be confused with the ind-object "$\varinjlim_{m,n} W_n^m$" from Proposition 23.9!

Lemma 25.2. (a) The Artin-Hasse exponential induces a group homomorphism $\widehat{W} \to \mathbb{G}_{m,k}$, $\underline{x} \mapsto E(\underline{x}, 1)$.
(b) For all $\underline{x} \in W(R)$ and $\underline{y} \in \widehat{W}(R)$, we have $E\big((V\underline{x}) \cdot \underline{y}, 1\big) = E\big(\underline{x} \cdot (F\underline{y}), 1\big)$.
(c) For all $n \geq 1$, all $\underline{x}, \underline{x}' \in W(R)$ with the same image in $W_n(R)$, and all $\underline{y} \in \widehat{W}(R)$ such that $F^n\underline{y} = 0$, we have $E(\underline{x} \cdot \underline{y}, 1) = E(\underline{x}' \cdot \underline{y}, 1)$.

Proof. (a) By definition $E(\underline{x}, t) = \prod_{n \geq 0} F(x_n t^{p^n}) \in 1 + t\mathbb{Z}[\underline{x}][[t]]$, where $F(t) = 1 - t \pm \cdots \in 1 + t\mathbb{Z}_{(p)}[[t]]$. Thus for any $\underline{x} \in \widehat{W}(R)$ the series $E(\underline{x}, t)$ is actually a polynomial in t with constant term 1. In particular it can be evaluated at $t = 1$, yielding an element $E(\underline{x}, 1) \in \mathbb{G}_m(R)$. Thus the morphism in question is defined, and it is a homomorphism because E itself defines a group homomorphism from $W = W_k$ to the multiplicative group scheme $\Lambda_k =$ "$1 + t\mathbb{A}_k^1[[t]]$".

(b) follows from Proposition 21.1 (g) by setting $t = 1$.

(c) By assumption $\underline{x} - \underline{x}'$ maps to zero in $W_n(R)$, so it must be of the form $\underline{x} - \underline{x}' = V^n\underline{z}$ for some $\underline{z} \in W(R)$. Thus $\underline{x} = \underline{x}' + V^n\underline{z}$. We deduce that

$$E\big(\underline{x}\underline{y}, 1\big) = E\big((\underline{x}' + V^n\underline{z})\underline{y}, 1\big) = E\big(\underline{x}'\underline{y} + (V^n\underline{z})\underline{y}, 1\big) = E\big(\underline{x}'\underline{y}, 1\big) \cdot E\big((V^n\underline{z})\underline{y}, 1\big),$$

where we have also used the distributive law in W, Lemma 25.1, and the homomorphy of E. But (b) implies that the last factor is

$$E\big((V^n\underline{z})\underline{y}, 1\big) = E(\underline{z}(F^n\underline{y}), 1) = 1,$$

since $F^n\underline{y} = 0$ by assumption. □

Theorem 25.3. For all $n, m \geq 1$ there is a well-defined nondegenerate bilinear morphism

$$W_n^m \times W_m^n \to \mathbb{G}_{m,k}, \;\; (\underline{x}, \underline{y}) \mapsto \langle \underline{x}, \underline{y} \rangle := E\big(\tau_n^m(\underline{x}) \cdot \tau_m^n(\underline{y}), 1\big),$$

and it satisfies the following relations:
(a) $\langle \underline{x}, \underline{y} \rangle = \langle \underline{y}, \underline{x} \rangle$,
(b) $\langle v\underline{x}, \underline{y} \rangle = \langle \underline{x}, f\underline{y} \rangle$,
(c) $\langle r\underline{x}, \underline{y} \rangle = \langle \underline{x}, i\underline{y} \rangle$,
(d) $\langle V\underline{x}, \underline{y} \rangle = \langle \underline{x}, F\underline{y} \rangle$,
(e) $\langle \xi\underline{x}, \underline{y} \rangle = \langle \underline{x}, \xi\underline{y} \rangle$ for all $\xi \in W(k)$.
In particular, its adjoint is a canonical isomorphism $W_n^m \xrightarrow{\sim} (W_m^n)^*$.

Proof. Lemmas 25.1 (b) and 25.2 (a) imply that the morphism is well-defined. To see that it is bilinear, consider any $\underline{x}, \underline{x}' \in W_n^m(R)$ and $\underline{y} \in W_m^n(R)$. Then $\tau_n^m(\underline{x}+\underline{x}')$ and $\tau_n^m(\underline{x})+\tau_n^m(\underline{x}')$, even though they might be different in $\widehat{W}(R)$, have the same image in $W_n(R)$. Thus using Lemma 25.2 (a) and (c) one directly computes that $\langle \underline{x} + \underline{x}', \underline{y} \rangle = \langle \underline{x}, \underline{y} \rangle + \langle \underline{x}', \underline{y} \rangle$, as desired.

The same reasoning with $\tau_n^m(\xi\underline{x})$ and $\xi \cdot \tau_n^m(\underline{x})$ works for (e), and with $\tau_n^m(r\underline{x})$ and $\tau_{n+1}^m(\underline{x})$ for $\underline{x} \in W_{n+1}^m(R)$ it works for (c). Part (b) results from the calculation

$$\begin{aligned} \langle v\underline{x}, \underline{y} \rangle \;\; &= \;\; E\big(\tau_{n+1}^m(v\underline{x}) \cdot \tau_m^{n+1}(\underline{y}), 1\big) \;\; = \;\; E\big((V\tau_n^m(\underline{x})) \cdot \tau_m^{n+1}(\underline{y}), 1\big) \\ &\overset{25.2\,(b)}{=} E\big(\tau_n^m(\underline{x}) \cdot (F\tau_m^{n+1}(\underline{y})), 1\big) \;\; = \;\; E\big(\tau_n^m(\underline{x}) \cdot \tau_m^n(f\underline{y}), 1\big) \;\; = \;\; \langle \underline{x}, f\underline{y} \rangle \end{aligned}$$

for any $\underline{x} \in W_n^m(R)$ and $\underline{y} \in W_m^{n+1}(R)$. Moreover, (a) is obvious, and (d) follows from (b) and (c) and the relations $V = rv$ and $F = fi$ from §22.

It remains to prove nondegeneracy, and for this we begin with the case $n = m = 1$. Since $W_1^1 = \boldsymbol{\alpha}_p$ is simple, it suffices to prove that the pairing is nontrivial. But in this case we have

$$\langle x, y \rangle \;\; = \;\; E\big(\tau_1^1(x) \cdot \tau_1^1(y), 1\big) \overset{20.7}{=} E\big(\tau_1^1(xy), 1\big) \;\; = \;\; F(xy) \;\; = \;\; 1 - xy \pm \ldots,$$

which is not identically 1 for (x, y) in $\boldsymbol{\alpha}_p \times \boldsymbol{\alpha}_p$, as desired.

The general case can be deduced from this in two ways. One way is to perform induction over n and m, by relating the short exact sequences from the beginning of §22 and their Cartier duals, using the adjunctions in (b) and (c), and then applying the five lemma. Another way is to first show that every non-zero subgroup scheme $G \subset W_n^m$ contains $i^{m-1}v^{n-1}(W_1^1)$. Indeed, this follows at once from Lemma 22.1 and the fact that G must possess a subgroup scheme isomorphic to $\boldsymbol{\alpha}_p \cong W_1^1$. By symmetry, it is then enough to show that $\langle -, - \rangle$ is non-trivial on $i^{m-1}v^{n-1}(W_1^1) \times W_m^n$, which follows from the special case $n = m = 1$ by (b) and (c). $\square$