Lecture 7

December 2, 2004
Notes by Ivo Dell'Ambrogio

§17 Group orders

Recall from Theorem 15.5 that every finite commutative group scheme possesses a unique and functorial decomposition

$$G = G_{rr} \oplus G_{r\ell} \oplus G_{\ell r} \oplus G_{\ell\ell}$$

where the direct summands are of reduced-reduced, reduced-local, local-reduced, and local-local type, respectively.

Theorem 17.1. (a) The group orders in the above decomposition are, respectively: prime to p for G_{rr}, and a power of p for $G_{r\ell}$, $G_{\ell r}$ and $G_{\ell\ell}$.

(b) ("Lagrange") $|G| \cdot \mathrm{id}_G = 0$.

Proof. The statements are invariant under base extension; hence we may assume that k is separably closed. Recall that the group order is multiplicative in any short exact sequence $0 \to G' \to G \to G'' \to 0$. Similarly, if the Lagrange equation holds for G' and G'', one easily shows that it also holds for G. Therefore both statements reduce to the case of simple G.

If G is also reduced, then it must be the constant group scheme associated to a simple finite commutative group, and therefore $G \cong \underline{\mathbb{Z}/\ell\mathbb{Z}}$ for a prime ℓ. Its Cartier dual is then $G^* \cong \mu_{\ell,k}$, which is reduced if and only if $\ell \neq p$. This determines the simple reduced group schemes up to isomorphism, and by Cartier duality also those of local-reduced type. Taking Theorem 16.3 into account, we deduce that the simple finite commutative group schemes over a separably closed field up to isomorphism are the following:

Type	Group	Order
reduced-reduced	$\underline{\mathbb{Z}/\ell\mathbb{Z}}$	$\ell \neq p$
reduced-local	$\underline{\mathbb{Z}/p\mathbb{Z}}$	p
local-reduced	$\mu_{p,k}$	p
local-local	$\alpha_{p,k}$	p

In each case G is annihilated by its order, and the proposition follows. ∎

§18 Motivation for Witt vectors

Let R be a complete discrete valuation ring with quotient field of characteristic zero, maximal ideal pR, and residue field $k = R/pR$. Then we can write all elements of R as power series in p. In fact, for any given (set theoretic) section $s : k \to R$ we have a bijection

$$\prod_{n=0}^{\infty} k \longrightarrow R, \quad (x_n) \longmapsto \sum_{n=0}^{\infty} s(x_n) \cdot p^n.$$

A natural problem is then to describe the ring structure of R in terms of the coefficients x_n. This of course depends on the choice of s, so the question is: How can this be done canonically? For the following we shall again assume that k is a perfect field.

Proposition 18.1. Let R be a complete noetherian local ring with perfect residue field k of characteristic p and maximal ideal $\mathfrak{m}$. Then there exists a unique section $i : k \to R$ with the equivalent properties:

(a) $i(xy) = i(x)i(y)$ for all $x, y \in k$,

(b) $i(x) = \lim_{n\to\infty} s(x^{p^{-n}})^{p^n}$ for any section s and any $x \in k$.

The image $i(x)$ is called the *Teichmüller representative of* x.

Proof. The main point is to show that the limit in (b) is well-defined. First notice that for all $n \geq 1$ and $x, y \in R$ we have

$$x \equiv y \bmod \mathfrak{m}^n \quad \Rightarrow \quad x^p \equiv y^p \bmod \mathfrak{m}^{n+1}.$$

This is because with $z := y - x \in \mathfrak{m}^n$ the binomial formula implies that

$$y^p - x^p = (z + x)^p - x^p \in (z^p, pz) \subset \mathfrak{m}^{n+1}.$$

By induction on n we deduce for all $n \geq 0$ and $x, y \in R$ that

$$x \equiv y \bmod \mathfrak{m} \quad \Rightarrow \quad x^{p^n} \equiv y^{p^n} \bmod \mathfrak{m}^{n+1}.$$

Note also that the assumptions imply that $R \cong \varprojlim_n R/\mathfrak{m}^n$.

Now consider any section $s\colon k \to R$. Then for all $x \in k$ and $n \geq 1$ we have $s(x^{p^{-n}})^p \equiv s(x^{p^{1-n}}) \bmod \mathfrak{m}$ and therefore $s(x^{p^{-n}})^{p^n} \equiv s(x^{p^{1-n}})^{p^{n-1}} \bmod \mathfrak{m}^n$. This shows that the sequence in (b) converges. If $s' : k \to R$ is another section, we have $s(y) \equiv s'(y) \bmod \mathfrak{m}$ for all $y \in k$; hence $s(x^{p^{-n}})^{p^n} \equiv s'(x^{p^{-n}})^{p^n} \bmod \mathfrak{m}^{n+1}$ for all $x \in k$ and $n \geq 0$, and so the limits coincide. Thus we have proved (b), and to prove that (b) is equivalent to (a) one proceeds similarly. ☐

In order to reconstruct the ring R from k, the main problem is now to describe its additive structure in terms of i. Once this is done, the multiplication can be deduced from Proposition 18.1 (a) and the distributive law:

$$\Big(\sum_n i(x_n)p^n\Big) \cdot \Big(\sum_m i(y_m)p^m\Big) = \sum_{n,m} i(x_n y_m)p^{n+m}.$$

One may wonder here: Does the addition depend on further structural invariants of R, or is it given by universal formulae? A hint towards the second option is given by the fact that the addition in the ring of p-adic integers $\mathbb{Z}_p \subset R$ is already unique. Indeed the latter is the case, and the problem is solved by the so-called ring of Witt vectors. This solution actually turnes everything around and defines a natural ring structure on $\prod_{n=0}^{\infty} k$ without prior presence of R. Notice that this produces a ring of characteristic zero from a field of characteristic p!

The construction is related to the fact that, although the *additive* group of the ring of power series $k[[t]]$ is annihilated by p, its *multiplicative* group of 1-units $1 + t \cdot k[[t]]$ is torsion free! Thus some aspect of characteristic zero is present in characteristic p.

The strategy is to first use power series over $\mathbb{Q}$ to produce some formulae which—somewhat miraculously—turn out to be integral at p, and then to reduce these formulae mod p.

§19 The Artin-Hasse exponential

Recall the Möbius function defined for integers $n \geq 1$ by

$$\mu(n) = \begin{cases} (-1)^{(\text{number of prime divisors of } n)} & \text{if } n \text{ is square-free,} \\ 0 & \text{otherwise.} \end{cases}$$

It is also characterized by the basic property

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 19.1. In $1 + t \cdot \mathbb{Q}[[t]]$ we have the equality

$$\exp(-t) = \prod_{n \geq 1} (1 - t^n)^{\frac{\mu(n)}{n}},$$

where the factors are evaluated by the binomial series.

Proof. Taking logarithms the equality follows from the calculation

$$\begin{aligned}\sum_{n\geq 1}\frac{\mu(n)}{n}\log(1-t^n) &= \sum_{n\geq 1}\frac{\mu(n)}{n}\sum_{m\geq 1}\Big(-\frac{t^{nm}}{m}\Big)\\ &\overset{d=nm}{=} -\sum_{d\geq 1}\Big(\sum_{n|d}\mu(n)\Big)\frac{t^d}{d} \;=\; -t.\end{aligned}$$

□

Note. On the right hand side above, all denominators come from the powers of $\frac{\mu(n)}{n}$ in the binomial series. The following definition will separate the p-part of these denominators from the non-p-part. Observe that the localization $\mathbb{Z}_{(p)}$ is the ring of rational numbers without p in the denominator.

Definition. $F(t) := \prod_{p\nmid n}(1-t^n)^{\frac{\mu(n)}{n}} \in 1 + t\cdot\mathbb{Z}_{(p)}[[t]]$.

Lemma 19.2. $F(t) = \exp\Big(-\sum_{m\geq 0}\frac{t^{p^m}}{p^m}\Big)$.

Note. Thus we have the interesting situation that $F(t)$ is a power series without p in the denominators, but its logarithm has only powers of p in the denominators, while of course the logarithm and exponential series have all primes in their denominators. Insofar the definition of $F(t)$ is not as artificial as it might seem.

Proof. We again apply the logarithm:

$$\begin{aligned}\log F(t) &= \sum_{p\nmid n}\frac{\mu(n)}{n}\cdot\log(1-t^n)\\ &\overset{19.1}{=} -t - \sum_{p|n}\frac{\mu(n)}{n}\cdot\log(1-t^n)\\ &\overset{n=mp}{=} -t - \sum_{m}\frac{\mu(mp)}{mp}\cdot\log(1-t^{mp})\\ &\overset{(*)}{=} -t + \frac{1}{p}\sum_{p\nmid m}\frac{\mu(m)}{m}\log(1-t^{mp})\\ &= -t + \frac{1}{p}\log F(t^p)\end{aligned}$$

where $(*)$ uses the observation that if $p|m$, then mp is not square free and hence $\mu(mp) = 0$. The lemma follows by iterating this formula. □

Lemma 19.3. There exist unique polynomials $\psi_n \in \mathbb{Z}[x,y]$ such that:

$$F(xt)\cdot F(yt) \;=\; \prod_{n\geq 0} F\big(\psi_n(x,y)\cdot t^{p^n}\big).$$

Proof. Since the power series $F(t)$ is congruent to $1-t \mod t^2$ and has coefficients in $\mathbb{Z}_{(p)}$, by successive approximation we find unique polynomials $\lambda_d \in \mathbb{Z}_{(p)}[x,y]$ such that

$$F(xt)\cdot F(yt) \;=\; \prod_{d\geq 1} F\big(\lambda_d(x,y)\cdot t^{d}\big).$$

Taking logarithm on both sides and using Lemma 19.2, this formula is equivalent to

$$\begin{aligned} -\sum_{m\geq 0}(x^{p^m}+y^{p^m})\cdot\frac{t^{p^m}}{p^m} \;&=\; -\sum_{d\geq 1}\sum_{m\geq 0}\lambda_d(x,y)^{p^m}\cdot\frac{t^{dp^m}}{p^m} \\ &=\; -\sum_{e\geq 1}\Bigg(\sum_{\substack{m\geq 0\\ p^m|e}}\frac{\lambda_{e/p^m}(x,y)^{p^m}}{p^m}\Bigg)\cdot t^e. \end{aligned}$$

Comparing coefficients, this shows that each λ_e is given recursively as a polynomial over $\mathbb{Z}[\frac{1}{p}]$ in x, y, and $\lambda_{e'}$ for certain $e'<e$. Thus by induction on e we deduce that λ_e lies in $\mathbb{Z}[\frac{1}{p}][x,y]$. Since a priori it is also in $\mathbb{Z}_{(p)}[x,y]$, we find that actually $\lambda_e \in \mathbb{Z}[x,y]$.

Moreover, suppose that $\lambda_e \neq 0$ for some $e \geq 1$ which is not a power of p. Then there exists a smallest e with this property, and for this e the above formula shows that λ_e is a $\mathbb{Q}$-linear combination of $\lambda_{e/p^m}^{p^m}$ for $m>0$ with $p^m|e$. But all those terms vanish by the minimality of e, yielding a contradiction. Therefore $\lambda_e = 0$ whenever e is not a power of p, and so the lemma follows with $\psi_n := \lambda_{p^n}$. □

Now for any ring R we set

$$\Lambda_R \;:=\; \prod_{d\geq 1}\mathbb{A}^1_R \;=\; \operatorname{Spec} R[U_1,U_2,\cdots].$$

This is a scheme over R, only not of finite type. Identifying sequences $(u_1,u_2,\ldots)$ with power series $1+u_1t+u_2t^2+\ldots$ turns $\Lambda_R \cong$ "$1+t\cdot\mathbb{A}^1_R[[t]]$" into a commutative group scheme over R by the usual multiplication of power series

$$(1+u_1t+u_2t^2+\ldots)\cdot(1+v_1t+v_2t^2+\ldots) = 1+(u_1+v_1)t+(u_2+u_1v_1+v_2)t^2+\ldots.$$

Lemma 19.3 suggests that products of the form $\prod_{n\geq 0} F(x_n \cdot t^{p^n})$ form a subgroup of Λ_R. For any ring R we let

$$W_R := \prod_{n\geq 0} \mathbb{A}^1_R = \operatorname{Spec} R[X_0, X_1, \ldots]$$

and write points in it in the form $\underline{x} = (x_0, x_1, \ldots)$.

Definition. The *Artin-Hasse exponential* is the morphism E given by

$$\mathrm{W}_{\mathbb{Z}_{(p)}} \longrightarrow \Lambda_{\mathbb{Z}_{(p)}}, \quad \underline{x} \mapsto E(\underline{x}, t) := \prod_{n\geq 0} F(x_n \cdot t^{p^n}).$$

Proposition 19.4. There exists unique polynomials $s_n \in \mathbb{Z}[x_0, \ldots, x_n, y_0, \ldots, y_n]$ such that $E(\underline{x}, t) \cdot E(\underline{y}, t) = E(\underline{s}(\underline{x}, \underline{y}), t)$ with $\underline{s} = (s_0, s_1, \ldots)$. Moreover, the morphism $\underline{s} \colon \mathrm{W}_\mathbb{Z} \times \mathrm{W}_\mathbb{Z} \to \mathrm{W}_\mathbb{Z}$ defines the structure of a commutative group scheme over $\mathbb{Z}$.

Proof. The first part is proved by successive approximation using Lemma 19.3. For the "moreover" part we must produce the unit section and the inversion morphism of $W_\mathbb{Z}$. The former is defined as $\underline{0} = (0, 0, \ldots)$ and satisfies $E(\underline{0}, t) = 1$. For the latter we first show by explicit calculation that

$$F(t)^{-1} = \begin{cases} F(-t) & \text{if } p \neq 2, \\ \prod_{n\geq 0} F\big(-t^{p^n}\big) & \text{if } p = 2, \end{cases}$$

taking logarithms and using Lemma 19.2. By successive approximation we then find a unique morphism $\underline{i} \colon W_\mathbb{Z} \to W_\mathbb{Z}$ satisfying $E(\underline{x}, t)^{-1} = E(\underline{i}(\underline{x}), t)$. It remains to verify the group axioms for $\underline{s}$, $\underline{0}$, and $\underline{i}$, and that in turn can be done over $\mathbb{Z}_{(p)}$. But it is clear by construction that the Artin-Hasse exponential defines a closed embedding $E : \mathrm{W}_{\mathbb{Z}_{(p)}} \hookrightarrow \Lambda_{\mathbb{Z}_{(p)}}$. Thus by the above formulas relating E with $\underline{s}$, $\underline{0}$, and $\underline{i}$ the desired group axioms follow at once from those in $\Lambda_{\mathbb{Z}_{(p)}}$, finishing the proof. □

The next proposition will not be needed in the sequel, but it serves as an illustration of what is going on here.

Proposition 19.5. The morphism below is an isomorphism of group schemes:

$$\prod_{p\nmid m} \mathrm{W}_{\mathbb{Z}_{(p)}} \xrightarrow{\sim} \Lambda_{\mathbb{Z}_{(p)}}, \quad (\underline{x}_m)_m \mapsto \prod_{p\nmid m} E(\underline{x}_m, t^m) = \prod_{\substack{p\nmid m \\ n\geq 0}} F(x_{mn} \cdot t^{mp^n}).$$

Proof. Easy, using Proposition 19.4. □

Note. One can show that $\mathrm{W}_{\mathbb{Z}_{(p)}}$ is an indecomposable group scheme over $\mathbb{Z}_{(p)}$; hence by Proposition 19.5 it can be regarded as the unique indecomposable component of $\Lambda_{\mathbb{Z}_{(p)}}$ up to isomorphism. This illustrates a certain canonicity of $\mathrm{W}_{\mathbb{Z}_{(p)}}$, independent of the precise choice of F in its construction.