Algebraic Number Theory 3 – Formal groups WS 2016/17

Prof. Dr. Ulrich Görtz

Dr. Heer Zhao

Problem sheet 7

Due date: Dec. 14, 2016

Problem 25

Consider the following system of equations in $X_1, \cdots, X_{n-1}$:

$$\begin{cases} X_i = X_{n-i}, & \text{for } i = 1, \cdots, n-1; \\ \binom{i+j}{j} X_{i+j} = \binom{j+k}{j} X_{j+k}, & \forall i, j, k \geqslant 1 \text{ with } i + j + k = n. \end{cases} \tag{0.1}$$

Let $\mathcal{A}b$ (resp. $\mathcal{S}et$) be the category of abelian groups (resp. sets). Show that the functor

$$F : \mathcal{A}b \to \mathcal{S}et, \quad A \mapsto S_A,$$

where S_A denotes the set of solutions of the system (0.1) of equations in A^{n-1}, is representable by a finitely generated abelian group M.

Problem 26

Let $\ell_1, \cdots, \ell_{n-1}$ be integers satisfying

$$\sum_{i=1}^{n-1} \binom{n}{i} \ell_i = v(n) := \begin{cases} p, & \text{if } n = p^r \text{ for some prime } p \text{ and } r > 0; \\ 1, & \text{otherwise.} \end{cases}$$

Let $\varphi : \mathbb{Z} \to M$ be the group homomorphism (whose existence is guaranteed by Yoneda's Lemma) corresponding to the morphism of functors

$$\operatorname{Hom}_{\mathcal{A}b}(M, -)(A) = \operatorname{Hom}_{\mathcal{A}b}(M, A) = S_A \to A = \operatorname{Hom}_{\mathcal{A}b}(\mathbb{Z}, -)(A),$$
$$(a_1, \cdots, a_{n-1}) \mapsto \sum_{i=1}^{n-1} \ell_i a_i.$$

Show that the following statements are equivalent.

(1) The homomorphism φ is an isomorphism with inverse ψ corresponding to

$$A = \mathrm{Hom}_{\mathcal{A}b}(\mathbb{Z}, -)(A) \to \mathrm{Hom}_{\mathcal{A}b}(M, -)(A) = \mathrm{Hom}_{\mathcal{A}b}(M, A) = S_A,$$
$$a \mapsto \left(v(n)^{-1}\binom{n}{1}a, \cdots, v(n)^{-1}\binom{n}{n-1}a \right).$$

(2) The homomorphism φ is surjective.

(3) The base change $\varphi_{\mathbb{F}_p} := \varphi \otimes_{\mathbb{Z}} \mathbb{F}_p : \mathbb{F}_p \to M \otimes_{\mathbb{Z}} \mathbb{F}_p$ is surjective for every prime number p.

(4) $S_{\mathbb{F}_p} = \mathrm{Hom}_{\mathcal{A}b}(M, \mathbb{F}_p)$ is a 1-dimensional $\mathbb{F}_p$-vector space for every prime number p.

Now assume that the above properties hold. Conclude that for every abelian group A,

$$S_A = \left\{ \left(v(n)^{-1}\binom{n}{i}a \right)_i ; \ a \in A \right\}.$$

(This is the statement used in our proof of Lazard's Key Lemma.)

Hint: Check that $\psi \circ \varphi = 1_{\mathbb{Z}}$, in particular both φ and $\varphi_{\mathbb{F}_p}$ are injective; this is useful in proving (2) $\Rightarrow$ (1) and (4) $\Rightarrow$ (3).

For (3) $\Leftrightarrow$ (2), note that $\mathrm{coker}(\varphi)$ is finitely generated and that a finitely generated abelian group A vanishes if and only if $A \otimes_{\mathbb{Z}} \mathbb{F}_p = 0$ for all p (why?).

Remark: Statement (4) is a problem of linear algebra over $\mathbb{F}_p$, which is relatively easy to check. We omit the proof that (4) (and hence (1)) always holds here; see Chapter I, Section 4.2 (in particular 4.2.4 and 4.2.5) of Hazewinkel's book "Formal groups and applications".

Problem 27

Let k be a separably closed field of positive characteristic p, G a 1-dimensional (commutative) formal group law over k and $f(X) := [p]_G$. Note that $f'(0) = 0$. Suppose that $f(X) \neq 0$, then $f(X) = g(X^{p^r})$ for a unique $g(X) \in k[[X]]$ with $g'(0) \neq 0$ by Problem 24. Show that G is isomorphic to a formal group law H over k with $[p]_H = X^{p^r}$.

Hint: As usual, modify $f(X)$ degree by degree and then pass to the limit. We need two kinds of modifications. If $f(X) \equiv aX^{p^r} \bmod \deg 2p^r$, use $h(X) = bX$ for suitable b to produce a formal group law

$$H(X,Y) := h(G(h^{-1}(X), h^{-1}(Y))),$$

such that $[p]_H(X) \equiv X^{p^r} \bmod \deg 2p^r$. If

$$f(X) \equiv X^{p^r} + aX^{kp^r} \bmod \deg (k+1)p^r$$

for some $k \geqslant 2$, use $h(X) = T - bT^k$ for suitable b to produce a formal group law

$$H(X,Y) := h(G(h^{-1}(X), h^{-1}(Y))),$$

such that $[p]_H(X) \equiv X^{p^r} \bmod \deg (k+1)p^r$. The assumption that k is separably closed is used to guarantee the existence of b.

Problem 28

Let R be a ring, G an n-truncated formal group law over R. Show that G extends to a formal group law over R.