A SIMPLE CONSTRUCTION OF THE FIELD OF WITT VECTORS.[1]

V.V.FOCK

Abstract. We present a short, hopefully pedagogical construction of the field and ring of Witt vectors. We are going to define a binary operation on polynomials of one variable modifying the definition of a resultant.

Introduction. Witt vectors form a field of characteristic 0 constructed out of a field of characteristic p. This construction suggested by E. Witt [1] in 1936 generalizes the field $\mathbb{Q}_p$ of p-adic rationals. His construction has a reputation to be complicated and counter-intuitive. We suggest a very concise version of construction of Witt vectors. It is inspired by a paper by D.Kaledin [2] who observed a relation between Witt vectors and the tame symbol in disguise of the so-called Japanese cocycle.

In the wikipedia article on Witt vectors it is indicated that "they have a highly non-intuitive structure". The aim of this note is to refute this claim.

Convolution. We are going to define a binary operation on polynomials of one variable modifying the definition of a resultant.

Let $f(t) = 1 + a_1 t + \cdots$ and $g(t) = 1 + b_1 t + \cdots$ belong to the multiplicative semi-group $1 + t\mathbb{F}[t]$ of polynomials with coefficients in a field $\mathbb{F}$ and the constant term equal to 1. Define a *convolution* $f \star g$ as a polynomial with the constant term 1 and having as roots the products of one root of f and one of g. In other words, suppose that $f(t) = \prod_i (1 - \lambda_i t)$ and $g(t) = \prod_j (1 - \mu_j t)$ with $\lambda_i, \mu_j \in \bar{\mathbb{F}}$. Then

$$f \star g\,(t) = \prod_{ij} (1 - t\lambda_i \mu_j) = \prod_i g(\lambda_i t) = \prod_j f(\mu_j t).$$

To give an equivalent definition, consider the ring $\mathbb{F}[x, y]/(f(x)) + (g(y))$ and denote by $\hat{x}^{-1}$ and $\hat{y}^{-1}$ the multiplication in this ring by x^{-1} and y^{-1}, respectively. In the standard basis they are given by matrices with entries in $\mathbb{F}$. Then

$$f \star g\,(t) = \det(1 - t\hat{x}^{-1}\hat{y}^{-1}).$$

Date: March 03 2024.

[1]The paper was submitted to arxiv, but was rejected for the lack or originality.

In this definition it is explicit that the coefficients of $f\star g$ are polynomial functions of those of f and g.

The third definition works for $\mathbb{F}=\mathbb{C}$ and shows the relation to the tame symbol. Consider a curve γ around zero on the complex plane sufficiently small in order not to surround any root of $f(z)$. The convolution can be defined by the formula

$$f\star g\,(t)=\{f(z),g(t/z)\}_\gamma=\exp(\frac{1}{2\pi i}\int_\gamma \ln f(z)d\ln g(t/z))$$

valid for t so small that all roots of $g(t/z)$ are inside the curve γ.

The convolution enjoys the following properties obvious from the definitions:

A. $\deg(f\star g)=\deg f\deg g$,
B. $f\star 1=1$,
C. $f\star(1-t)=f$,
D. $(1-at)\star(1-bt)=(1-abt)$,
E. $f\star g=g\star f$,
F. $f\star(g_1g_2)=(f\star g_1)(f\star g_2)$.

These three properties imply that the semi-group $1+t\mathbb{F}[t]$ is a commutative semi-ring with respect to the multiplication as a semi-ring addition and convolution as a semi-ring multiplication. The multiplicativity property F is just the expression of the distributive law of the semi-ring.

The following property is also an easy consequence of the definition:

G. The set $1+t^n\mathbb{F}[t]$ is an ideal.

This property implies that the convolution can be extended to the group of formal power series $1+t\mathbb{F}[[t]]$ providing it with a ring structure. This ring is called the *universal Witt ring* and is denoted by $W(\mathbb{F})$.

Witt vectors. The aim of this paragraph is to give a concise definition of the Witt ring.

For that we need just another property of the universal Witt ring obviously following from the definition of the convolution:

H. The set $1+t^n\mathbb{F}[[t^n]]$ is also an ideal.

Let $\mathbb{F}$ be a field of characteristic p and let $W(\mathbb{F})$ be the corresponding universal Witt ring.

Define the *Witt ring* $W_\mathbb{F}$ as a quotient

$$W_\mathbb{F}=W(\mathbb{F})/\prod_{n>1|(n,p)=1}(1+t^n\mathbb{F}[[t^n]])$$

Here we used the property H and denoted the sum of ideals multiplicatively since it corresponds to the product of the series.

Observe that any element of the group $1 + t\mathbb{F}[[t]]$ can be presented either as a sum $1+\alpha_1 t+\alpha_2 t^2+\cdots$ or as a product $(1-a_1 t)(1-a_2 t^2)(1-a_3 t^3)\cdots$.

Using the latter presentation the elements of the ring $W_{\mathbb{F}}$ can be uniquely represented as products

$$f(t) = \prod_{i=0}^{\infty}(1 - a_i t^{p^i})$$

In this presentation certain properties of the Witt vectors become obvious. In particular, it follows from the property D that the correspondence $a \mapsto (1 - at)$ gives an embedding of multiplicative groups $\mathbb{F}^\times \to W_{\mathbb{F}}^\times$. The images of the elements of $\mathbb{F}^\times$ are called their *Teichmüller representatives.* It is also obvious that the ring multiplication by p in the ring $W_{\mathbb{F}}$ amounts to the shift of the coefficients a_i composed with the Frobenius automorphism:

$$\prod_{i=0}^{\infty}(1 - a_i t^{p^i}) \mapsto \prod_{i=1}^{\infty}(1 - a_{i-1}^p t^{p^i})$$

This property allows to identify the field of fractions of the ring $W_{\mathbb{F}}$ with the expressions of the form

$$\prod_{i=N}^{\infty}(1 - a_i t^{p^i})$$

with possibly negative N.

Recall that for a field $\mathbb{F}_p$ of p elements the ring $W_{\mathbb{F}}$ coincides with the ring $\mathbb{Z}_p$ of p-adic integers.

Relation to the standard definition of the Witt vectors. Consider the ring of formal series $\mathbb{C}[[t]]^{+\circ}$ with respect to addition and coefficentwise (Hadamard) multiplication denoted by $\circ$ defined as

$$(\sum_{k=0}^{\infty} a_k t^k) \circ (\sum_{k=0}^{\infty} b_k t^k) = \sum_{k=0}^{\infty} a_k b_k t^k$$

Clearly this ring is just a direct sum of infinitely many copies of the ring $\mathbb{C}$.

The map $f \mapsto -f'/f$ gives an isomorphism between the rings $(1+\mathbb{C}[[t]])^{\cdot\star}$ and $\mathbb{C}[[t]]^{+\circ}$. Indeed

$$(-f'/f)\circ(-g'/g) = \left(\sum_{k=1}^{\infty}(\sum_i \lambda_i^k)t^{k-1}\right)\circ\left(\sum_{k=0}^{\infty}(\sum_j \mu_j^k)t^{k-1}\right) =$$

$$= \left(\sum_k(\sum_{ij}\lambda_i^k\mu_j^k)t^{k-1}\right) = -(f\star g)'/(f\star g),$$

and obviously

$$-f'/f - g'/g = -(fg)'/(fg).$$

In the explicit coordinates we have

$$\prod(1-a_it^i) \mapsto \sum_i\sum_k a_i^k t^{ik-1} = \sum_l\sum_{i|l} i a_i^{l/i} t^{l-1}.$$

The expressions

$$S_l(a_1,a_2,\ldots) = \sum_{i|l} i a_i^{i/l}$$

are called the *universal Witt polynomials*. We see that each of the Witt polynomials gives a homomorphism from the universal Witt ring to the ring of complex numbers and a collection of all such polynomials gives an isomorphism of the universal Witt ring to the infinite sum of complex numbers. The standard construction uses this isomorphism to define the ring structure in terms of the coefficients a_i. Then one proves that the product and the sum and in fact given by algebraic expressions with integer coefficients and thus are defined over any field.

References

[1] E. Witt, *Zyklische Körper und Algebren der Characteristik p vom Grad p^n,* Journal für die Reine und Angewandte Mathematik, 1937 (176): 126–140,

[2] D. Kaledin, *Universal Witt vectors and the Japanese cocycle,* Moscow Math. J. 12 (2012), 593–604.

IRMA, Université de Strasbourg