From Lang's "Algebra"

over **Z**, i.e. the group generated by σ and σ^u is free abelian of rank 2. In particular $\{\sigma\}$ and $\{\sigma, \sigma^u\}$ have the same fixed field k.

Witt vectors

46. Let $x_1, x_2, \ldots$ be a sequence of algebraically independent elements over the integers **Z**. For each integer $n \geqq 1$ define

$$x^{(n)} = \sum_{d|n} d x_d^{n/d}.$$

Show that x_n can be expressed in terms of $x^{(d)}$ for $d|n$, with rational coefficients.

Using vector notation, we call $(x_1, x_2, \ldots)$ the Witt components of the vector x, and call $(x^{(1)}, x^{(2)}, \ldots)$ its **ghost** components. We call x a **Witt vector**.

Define the power series

$$f_x(t) = \prod_{n \geqq 1} (1 - x_n t^n).$$

Show that

$$-t \frac{d}{dt} \log f_x(t) = \sum_{n \geqq 1} x^{(n)} t^n.$$

[By $\frac{d}{dt} \log f(t)$ we mean $f'(t)/f(t)$ if $f(t)$ is a power series, and the derivative $f'(t)$ is taken formally.]

If x, y are two Witt vectors, define their sum and product componentwise *with respect to the ghost components*, i.e.

$$(x + y)^{(n)} = x^{(n)} + y^{(n)}.$$

What is $(x + y)_n$? Well, show that

$$f_x(t) f_y(t) = \prod (1 + (x + y)_n t^n) = f_{x+y}(t).$$

Hence $(x + y)_n$ is a polynomial with integer coefficients in $x_1, y_1, \ldots, x_n, y_n$. Also show that

$$f_{xy}(t) = \prod_{d, e \geqq 1} (1 - x_d^{m/d} y_e^{m/e} t^m)^{de/m}$$

where m is the least common multiple of d, e and d, e range over all integers $\geqq 1$. Thus $(xy)_n$ is also a polynomial in $x_1, y_1 \ldots, x_n, y_n$ with integer coefficients. The above arguments are due to Witt (oral communication) and differ from those of his original paper.

If A is a commutative ring, then taking a homomorphic image of the polynomial ring over **Z** into A, we see that we can define addition and multiplication of Witt vectors with components in A, and that these Witt vectors form a ring $W(A)$. Show that W is a functor, i.e. that any ring homomorphism φ of A into a commutative ring A' induces a homomorphism $W(\varphi): W(A) \to W(A')$.

V is called Verschiebung (the German for "shift").

47. Let p be a prime number, and consider the projection of $W(A)$ on vectors whose components are indexed by a power of p. Now use the log to the base p to index these components, so that we write x_n instead of x_{p^n}. For instance, x_0 now denotes what was x_1 previously. For a Witt vector $x = (x_0, x_1, \ldots, x_n, \ldots)$ define

$$Vx = (0, x_0, x_1, \ldots) \quad \text{and} \quad Fx = (x_0^p, x_1^p, \ldots).$$

Thus V is a shifting operator. We have $V \circ F = F \circ V$. Show that

$$(Vx)^{(n)} = px^{(n-1)} \quad \text{and} \quad x^{(n)} = (Fx)^{(n-1)} + p^n x_n.$$

Also from the definition, we have

$$x^{(n)} = x_0^{p^n} + px_1^{p^{n-1}} + \cdots + p^n x_n.$$

48. Let k be a field of characteristic p, and consider $W(k)$. Then V is an additive endomorphism of $W(k)$, and F is a ring homomorphism of $W(k)$ into itself. Furthermore, if $x \in W(k)$ then

$$px = VFx.$$

If $x, y \in W(k)$, then $(V^i x)(V^j y) = V^{i+j}(F^{p^j}x \cdot F^{p^i}y)$. For $a \in k$ denote by $\{a\}$ the Witt vector $(a, 0, 0, \ldots)$. Then we can write symbolically

$$x = \sum_{i=0}^{\infty} V^i\{x_i\}.$$

Show that if $x \in W(k)$ and $x_0 \neq 0$ then x is a unit in $W(k)$. *Hint*: One has

$$1 - x\{x_0^{-1}\} = Vy$$

and then

$$x\{x_0^{-1}\} \sum_0^{\infty} (Vy)^i = (1 - Vy) \sum_0^{\infty} (Vy)^i = 1.$$

49. Let n be an integer $\geqq 1$ and p a prime number again. Let k be a field of characteristic p. Let $W_n(k)$ be the ring of truncated Witt vectors $(x_0, \ldots, x_{n-1})$ with components in k. We view $W_n(k)$ as an additive group. If $x \in W_n(k)$, define $\wp(x) = Fx - x$. Then $\wp$ is a homomorphism. If K is a Galois extension of k, and $\sigma \in G(K/k)$, and $x \in W_n(K)$ we can define σx to have component $(\sigma x_0, \ldots, \sigma x_{n-1})$. Prove the analogue of Hilbert's Theorem 90 for Witt vectors, and prove that the first cohomology group is trivial. (One takes a vector whose trace is not 0, and finds a coboundary the same way as in the proof of Theorem 10.1).

50. If $x \in W_n(k)$, show that there exists $\xi \in W_n(\bar{k})$ such that $\wp(\xi) = x$. Do this inductively, solving first for the first component, and then showing that a vector $(0, \alpha_1, \ldots, \alpha_{n-1})$ is in the image of $\wp$ if and only if $(\alpha_1, \ldots, \alpha_{n-1})$ is in the image of $\wp$. Prove inductively that if $\xi, \xi' \in W_n(k')$ for some extension k' of k and if $\wp\xi = \wp\xi'$ then $\xi - \xi'$ is a vector with components in the prime field. Hence the solutions of $\wp\xi = x$ for given $x \in W_n(k)$ all differ by the vectors with components in the prime field, and there are p^n such vectors. We define

$$k(\xi) = k(\xi_0, \ldots, \xi_{n-1}),$$