# Witt vectors

| | |
|---|---|
| Canonical name | WittVectors |
| Date of creation | 2013-03-22 15:14:31 |
| Last modified on | 2013-03-22 15:14:31 |
| Owner | alozano (2414) |
| Last modified by | alozano (2414) |
| Numerical id | 5 |
| Author | alozano (2414) |
| Entry type | Definition |
| Classification | msc 13K05 |
| Classification | msc 13J10 |
| Defines | Witt polynomials |

In this entry we define a commutative ring, the Witt vectors, which is particularly useful in number theory, algebraic geometry and other areas of commutative algebra. The Witt vectors are named after Ernst Witt.

**Theorem 1.** *Let $p$ be a prime and let $\mathbb{K}$ be a perfect ring of characteristic $p$. There exists a unique* `http://planetmath.org/PRing`*strict $p$-ring $W(\mathbb{K})$ with residue ring $\mathbb{K}$.*

**Definition 1.** *Let $\mathbb{K}$ be a perfect ring of characteristic $p$. The unique* `http://planetmath.org/PR` *$p$-ring $W(\mathbb{K})$ with residue ring $\mathbb{K}$ is called the ring of Witt vectors with coefficients in $\mathbb{K}$.*

Next, we give an explicit construction of the Witt vectors.

**Definition 2.** *Let $p$ be a prime number and let $\{X_i\}_{i=0}^{\infty}$ be a sequence of indeterminates. The polynomials $W_n \in \mathbb{Z}[X_1, \ldots, X_n]$ given by:*

$$\begin{aligned} W_0 &= X_0, \\ W_1 &= X_0^p + pX_1, \\ W_n &= X_0^{p^n} + pX_1^{p^{n-1}} + \ldots + p^n X_n = \sum_{i=0}^{n} p^i X_i^{p^{n-i}}. \end{aligned}$$

*are called the Witt polynomials.*

**Proposition 1.** *Let $\{X_i\}$, $\{Y_i\}$ be two sequences of indeterminates. For every polynomial in two variables $Q(U,V) \in \mathbb{Z}[U,V]$ there exist polynomials $\{t_i\}_{i=0}^{\infty}$ in the variables $\{X_i\}$ and $\{Y_i\}$*

$$t_i \in \mathbb{Z}[\{X_i\}, \{Y_i\}]$$

*such that*

$$W_n(t_0, t_1, t_2, \ldots, t_n) = Q(W_n(X_0, X_1, \ldots), W_n(Y_0, Y_1, \ldots))$$

*for all $n \geq 0$.*

*Proof.* See [**?**], p. 40. □

Let $S_0,\ S_1,\ S_2, \ldots$ (resp. $P_0,\ P_1,\ P_2, \ldots$) be the polynomials $t_0,\ t_1,\ t_2, \ldots$ associated with $Q(U,V) = U + V$ (resp. $Q(U,V) = U \cdot V$) given by the previous proposition. We will use the polynomials $S_i$, $P_i$ to define the addition and multiplication in a new ring. In the following proposition, the notation $R^{\infty}$ stands for the set of all sequences $(r_1, r_2, \ldots)$ of elements in $R$.

**Theorem 2.** *Let $\mathbb{K}$ be a perfect ring of characteristic $p$. We define a ring $W = (\mathbb{K}^\infty, +, \cdot)$ where the addition and multiplication, for $k, h \in \mathbb{K}^\infty$, are defined by:*

$$k + h = (S_0(k,h), S_1(k,h), \ldots), \quad k \cdot h = (P_0(k,h), P_1(k,h), \ldots).$$

*Then the ring $W$ concides with $W(\mathbb{K})$, the ring of Witt vectors with coefficients in $\mathbb{K}$.*

**Definition 3.** *Let $\mathbb{K}$ be a perfect ring of characteristic $p$. We define the ring of Witt vectors of length $n$ (over $\mathbb{K}$) to be the ring $W_n(\mathbb{K}) = (\mathbb{K}^{n-1}, +, \cdot)$, where, for $k, h \in \mathbb{K}^{n-1}$:*

$$k + h = (S_0(k,h), \ldots, S_{n-1}(k,h)), \quad k \cdot h = (P_0(k,h), \ldots, P_{n-1}(k,h)).$$

It is clear from the definitions that:

$$W(\mathbb{K}) = \varprojlim W_n(\mathbb{K})$$

In words, $W(\mathbb{K})$ is the projective limit of the Witt vectors of finite length.

**Example 1.** Let $\mathbb{K} = \mathbb{F}_p$. Then $W_n(\mathbb{F}_p) = \mathbb{Z}/p^n\mathbb{Z}$. Thus:

$$W(\mathbb{F}_p) = \mathbb{Z}_p,$$

the ring of `http://planetmath.org/PAdicIntegers`$p$-adic integers.

# References


[1] J. P. Serre, *Local Fields*, Springer-Verlag, New York.