ON THE INTEGRALITY OF THE WITT POLYNOMIALS[1]

BY

ANDREAS DRESS AND CHRISTIAN SIEBENEICHER[2]

Consider, for example, the following covariant functors defined on the category **rings** of commutative rings with a unit element[3] and with values in **rings** :

$$\begin{array}{lcl} A & \mapsto & F(A) := A[X] \\ A & \mapsto & F(A) := A[X]/(X^2) \\ A & \mapsto & F(A) := A \times A \\ A & \mapsto & F(A) := A \otimes_{\mathbf{Z}} A \end{array}$$

These functors share the following property:

If p is a prime number and if $p \cdot A = 0$, then $p \cdot F(A) = 0$,
that is, $\quad$ char $A = p \Longrightarrow$ char $F(A) = p$.

Question: Do all functors from **rings** to **rings** share this property?

Answer: No.

The simplest **counterexample** known to us is based on the well known fact that every prime number p divides the binomial coefficient $\binom{p}{j}$ for all integers $j \in \{1, \ldots, p-1\}$.

Indeed, consider for an arbitrary ring A the subset

$$A_p^{(2)} := \{r_p(a,b) := (a, a^p + p \cdot b) \mid a, b \in A\} \subset A \times A.$$

[1]28. Séminaire Lotharingien de Combinatoire, 15–18 März 1992, Saint-Nabor, Ottrott.

[2]Universität Bielefeld, Fakultät für Mathematik, Postfach 10 01 31, D 33 501 Bielefeld. e–mail: dress@mathematik.uni-bielefeld.de sieben@mathematik.uni-bielefeld.de

[3]In the following all rings will be assumed to be commutative and to have a unit element, denoted by 1.

of the cartesian product $A \times A$ and observe that with

$$\begin{pmatrix} p \\ j \end{pmatrix}' := \frac{1}{p} \cdot \begin{pmatrix} p \\ j \end{pmatrix} \qquad (j \in \{1, \ldots, p-1\})$$

one has

$$\begin{array}{rcl} r_p(0,0) & = & (0,0) \in A_p^{(2)}, \\ r_p(1,0) & = & (1,1) \in A_p^{(2)}, \end{array}$$

as well as

$$\begin{aligned} & r_p(a_1, b_1) \pm r_p(a_2, b_2) = \\ & \quad = (a_1 \pm a_2, (a_1 \pm a_2)^p + p(b_1 \pm b_2 - \textstyle\sum_{j=1}^{p-1} (\pm 1)^j \begin{pmatrix} p \\ j \end{pmatrix}' \cdot a_1^{p-j} \cdot a_2^j)) \\ & \quad = r_p(a_1 \pm a_2, b_1 \pm b_2 - \textstyle\sum_{j=1}^{p-1} (\pm 1)^j \begin{pmatrix} p \\ j \end{pmatrix}' \cdot a_1^{p-j} \cdot a_2^j) \end{aligned}$$

and

$$\begin{aligned} & r_p(a_1, b_1) \cdot r_p(a_2, b_2) = \\ & \quad = (a_1 \cdot a_2, (a_1 \cdot a_2)^p + p \cdot (a_1^p \cdot b_2 + b_1 \cdot a_2^p + p \cdot b_1 \cdot b_2)) \\ & \quad = r_p(a_1 \cdot a_2, a_1^p \cdot b_2 + b_1 \cdot a_2^p + p \cdot b_1 \cdot b_2) \end{aligned}$$

for all $a_1, b_1, a_2, b_2 \in A$. So the subset $A_p^{(2)}$ is a sub–ring of the product ring $A \times A$ and the above formulae suggest to define quite formally a new addition and multiplication, say $\overset{p}{+}$ and $\overset{p}{\circ}$, on the set $A \times A$ by

$$(a_1, b_1) \overset{p}{+} (a_2, b_2) := (a_1 + a_2, b_1 + b_2 - \sum_{i=j}^{p-1} \begin{pmatrix} p \\ j \end{pmatrix}' \cdot a_1^{p-j} \cdot a_2^j)$$

and

$$(a_1, b_1) \overset{p}{\circ} (a_2, b_2) := (a_1 \cdot a_2, a_1^p \cdot b_2 + b_1 \cdot a_2^p + p \cdot b_1 \cdot b_2),$$

so that the map

$$r_p : A \times A \to A \times A \qquad (a, b) \mapsto r_p(a, b)$$

becomes a homomorphism from $(A \times A, \overset{p}{+}, \overset{p}{\circ})$ into the product–ring $A \times A$.

Obviously, if A has no p–torsion, the homomorphism r_p maps $(A \times A, \overset{p}{+}, \overset{p}{\circ})$ isomorpically onto $A_p^{(2)}$, which establishes in particular that $(A \times A, \overset{p}{+}, \overset{p}{\circ})$ is indeed a ring for such A. But even if A has p–torsion, in which case the map r_p is no more injective, $(A \times A, \overset{p}{+}, \overset{p}{\circ})$ is a ring. This can be verified either by direct computation or by using a surjective homomorphism from some appropriate p–torsion free ring, e.g. some polynomial ring over $\mathbf{Z}$, onto the ring A.

In other words, the above construction defines a functor

$$\begin{gathered}\mathbf{W}_{\mathbf{C}_p} : \mathbf{rings} \ \to \mathbf{rings} \\ A \mapsto \mathbf{W}_{\mathbf{C}_p}(A) := (A \times A, \overset{p}{+}, \overset{p}{\circ}) \\ (h : A \to A') \mapsto (\mathbf{W}_{\mathbf{C}_p}(h) : A \times A \to A' \times A' \quad (a,b) \mapsto (h(a), h(b)))\end{gathered}$$

for which there exists a canonical natural transformation

$$\begin{array}{rcl}\Phi : \mathbf{W}_{\mathbf{C}_p} & \to & \mathbf{id} \times \mathbf{id} \\ \Phi(A) : \mathbf{W}_{\mathbf{C}_p}(A) \to A \times A & : & (a,b) \mapsto r_p(a,b).\end{array}$$

This functor provides a counter–example for the assumption made above, i.e. if A is a ring for which $p \cdot A = 0$, then $p \cdot \mathbf{W}_{\mathbf{C}_p}(A) \neq 0$:

Indeed the calculation

$$\begin{array}{rcl} r_p(p \circ (a,b)) & = & p \cdot r_p(a,b) \\ & = & (pa, pa^p + p^2 b) \\ & = & r_p(pa, (1 - p^{p-1})a^p + pb) \end{array}$$

shows that

$$p \circ (1,0) = (p, 1 - p^{p-1})$$

holds at least if A has no p–torsion, and therefore, as above, this identity must hold for all rings A.

Hence if char $A = p$, then for the unit element $(1,0)$ of $\mathbf{W}_{\mathbf{C}_p}(A)$ one has

$$p \circ (1,0) = (0,1) \neq (0,0).$$

More generally, E. Witt observed that for every ring A the subset

$$\{(a_1, a_1^2 + 2a_2, \ldots, \sum_{d|n} d \cdot a_d^{n/d}, \ldots) \mid a_1, a_2, \ldots \in A\}$$

of the infinite product ring $A^{\mathbf{N}}$, $\mathbf{N} = \{1,2,3,\ldots\}$ constitutes a sub–ring of $A^{\mathbf{N}}$ and that, as above, this allows to construct a functor

$$\mathbf{W} : \mathbf{rings} \ \to \mathbf{rings}$$

which is uniquely determined by the following properties:

- $\mathbf{W}(A) = A^{\mathbf{N}}$
- $\mathbf{W}(h : A \to A') = h^{\mathbf{N}} \ : \ (a_1, a_2, \ldots) \mapsto (h(a_1), h(a_2), \ldots)$

- for every $n \in \mathbf{N}$ one has a natural transformation

$$\begin{array}{rcl} \Phi_n : \mathbf{W} & \longrightarrow & \mathbf{id} \\ \Phi_n(A) : \mathbf{W}(A) \to A & : & (a_1, a_2, \dots) \mapsto \sum_{d|n} d \cdot a_d^{n/d} \end{array}$$

To understand these constructions from a structural rather than a purely computational point of view, consider even more generally a pro–finite group G and let $\mathcal{O}(G)$ denote the set of open subgroups of G. For every ring A, one considers the ring

$$A^{\mathcal{O}(G)/\sim} := \{f : \mathcal{O}(G) \to A \mid f(U) = f(V) \text{ if } U \overset{G}{\sim} V\}$$

of all functions $f : \mathcal{O}(G) \to A$ which are constant on G–conjugacy classes. Then the subset of all those maps $g : \mathcal{O}(G) \to A$ for which there exists some $f \in A^{\mathcal{O}(G)/\sim}$ such that

$$g(U) = \sum_{W \in \mathcal{O}(G)}{}' \# \mathrm{Fix}_U(G/W) \cdot f(W)^{(W:U)}$$

(where the symbol $\sum'$ is meant to indicate that for each conjugacy class of open subgroups W of G exactly one summand has to be taken and with $(W : U) := (G : U)/(G : W)$[4]) can be shown to be a sub–ring of $A^{\mathcal{O}(G)/\sim}$. As above, this allows to construct an associated functor $\mathbf{W}_G$ from **rings** to **rings** described in

Theorem 1:
Let G be a pro–finite group and let $\mathcal{O}(G)$ denote the set of open sub–groups of G. Then there exists a unique functor $\mathbf{W}_G : \mathbf{rings} \to \mathbf{rings}$ with the following properties:

- $\mathbf{W}_G(A) := A^{\mathcal{O}(G)/\sim}$,
- for every ring homomorphism $h : A \to A'$ one has

$$\mathbf{W}_G(h) : \mathbf{W}_G(A) \to \mathbf{W}_G(A') \; : \; f \mapsto h \circ f,$$

- for every open subgroup $U \in \mathcal{O}(G)$ one has a natural transformation

$$\Phi_U : \mathbf{W}_G \longrightarrow \mathbf{id},$$

  defined by

$$\Phi_U(A) : \mathbf{W}_G(A) \to A \; : \; f \mapsto \sum_{V \in \mathcal{O}(G)}{}' \# \mathrm{Fix}_U(G/V) \cdot f(V)^{(V:U)}.$$

[4] which is an integer whenever $\mathrm{Fix}_U(G/W)$ is non empty

Remarks:

(1) Witt's theorem presents the special case where G is the pro–finite completion $\hat{\mathbf{C}}$ of the infinite cyclic group $\mathbf{C}$.

(2) The functor $\mathbf{W}_{\mathbf{C}_p}$ considered in our first example is precisely the functor $\mathbf{W}_{\mathbf{C}_p}$ for G the cyclic group $\mathbf{C}_p$ with p elements.

Further results concerning this construction are:

Theorem 2:
With $\mathbf{F_p}$ the finite field with p elements, one has $p^n \cdot \mathbf{W}_G(\mathbf{F_p}) = \mathbf{0}$ if and only if $p \cdot \#G_p$ divides p^n, where G_p denotes a p–Sylow subgroup of G. In particular, if G_p is infinite, one has $p^n \cdot \mathbf{W}_G(\mathbf{F_p}) \neq \mathbf{0}$ for all $n \in \mathbf{N}$.

Theorem 3:
There exists a canonical isomorphism from $\mathbf{W}_G(\mathbf{Z})$ onto the (completed) Burnside ring[5] $\widehat{\Omega}(G)$. It has the following property: If for every positive integer $q \in \mathbf{N}$ and for every $U \in \mathcal{O}(G)$ one denotes by $C^0(U,q))$ the U–set of all continuous maps from U into the discrete set $\{1,\dots,q\}$ [6] and if $\mathrm{ind}_U^G(C^0(U,q))$ denotes the almost finite G–set induced from it,[7] then the canonical isomorphism maps every $f \in \mathbf{W}_G(\mathbf{Z})$ with $f(U) \geq 0$ for all $U \in \mathcal{O}(G)$ onto the disjoint union

$$[f] := \dot{\bigcup_{U \in \mathcal{O}(G)}}{}' \, \mathrm{ind}_U^G(C^0(U, f(U))),$$

taken over all conjugacy classes in $\mathcal{O}(G)$.

Remark:
Using this isomorphism the above formula in Theorem 1 for the natural transformation $\Phi_U(A)$ has a rather natural interpretation:
for any $f \in \mathbf{W}_G(\mathbf{Z})$ as in Theorem 3 the number of U–invariant elements in the almost finite G–set $[f]$ is precisely $\sum'_{V \in \mathcal{O}(G)} \#\mathrm{Fix}_U(G/V) \cdot f(V)^{(V:U)}$.
In other words, using the identification $\mathbf{W}_G(\mathbf{Z}) = \widehat{\Omega}(G)$, the homomorphism $\Phi_U(\mathbf{Z}) : \mathbf{W}_G(\mathbf{Z}) \to \mathbf{Z}$ coincides with the homomorphism $\varphi : \widehat{\Omega}(G) \to \mathbf{Z}$, induced by associating to each almost finite G–set the number of its U–invariant elements.

[5] that is the Grothendieck ring of those discrete G–spaces—called *almost finite G–sets*— where for every open subgroup $U \in \mathcal{O}(G)$ there are only finitely many points which are invariant under U.

[6] $C^0(U,q))$ is easily seen to be an almost finite U–set.

[7] For an almost finite U–set X we denote by $\mathrm{ind}_U^G(X)$ the almost finite G–set induced by X. It is the by definition the set of U–orbits $\overline{(g,x)}$ in the cartesian product $G \times X$ relative to the (free) U–action $U \times (G \times X) \to G \times X$ defined by $(u,(g,x)) \mapsto (gu^{-1}, ux)$ where of course $g_1 \cdot \overline{(g_2,x)} := \overline{(g_1 g_2, x)}$.

Theorem 4:

1. For every open subgroup $U \in \mathcal{O}(G)$ there are natural transformations
   - $F_U : \mathbf{W}_G \to \mathbf{W}_U$
   - $V_U : \mathbf{W}_U \to \mathbf{W}_G$

   where for every ring A
   - the map $F_U(A) : \mathbf{W}_G(A) \to \mathbf{W}_U(A)$ is a ring homomorphism,
   - the map $V_U(A) : \mathbf{W}_U(A) \to \mathbf{W}_G(A)$ is an additive homomorphism.
2. Using the identification from Theorem 3 $F_U(\mathbf{Z}) : \mathbf{W}_G(\mathbf{Z}) \to \mathbf{W}_U(\mathbf{Z})$ coincides with the restriction map $\mathrm{res}_U^G : \widehat{\Omega}(G) \to \widehat{\Omega}(U)$ and $V_U(\mathbf{Z}) : \mathbf{W}_U(\mathbf{Z}) \to \mathbf{W}_G(\mathbf{Z})$ coincides with the induction map $\mathrm{ind}_U^G : \widehat{\Omega}(U) \to \widehat{\Omega}(G)$.
3. The standard identities relating restriction and induction hold more generally for F and V, e.g. for any ring A and any $x \in \mathbf{W}_G(A)$ and $y \in \mathbf{W}_U(A)$ one has $x \cdot V_U(A)(y) = V_U(A)(F_U(A)(x) \cdot y)$ (Frobenius reciprocity) and for $U_1, U_2 \in \mathcal{O}(G)$ and $x \in \mathbf{W}_{U_1}(A)$ one can compute $F_{U_2}(A)(V_{U_1}(A)(x)) \in \mathbf{W}_{U_2}(A)$ according to an appropriate variant of the Mackey sub–group formula.

Remark:
In case $G = \hat{\mathbf{C}}$, the natural transformations F and V specialize to the well known *Frobenius* and *Verschiebung* maps defined for universal Witt vectors. Moreover, the well known identities relating the Frobenius and Verschiebung maps follow from the third assertion of Theorem 4 in this particular case.

To prove Witt's theorem as well as Theorems 1 to 4 one needs to show that certain rational numbers—like e.g. $\frac{1}{p}\binom{p}{j}$—are indeed integers. In the case $\frac{1}{p}\binom{p}{i}$ this, of course, can be shown by direct computation, but it can also be shown without any computation by realizing that $\frac{1}{p}\binom{p}{j}$ is the number of orbits of the action of the cyclic group $\mathbf{C}_p$ of order p on the set $\binom{\mathbf{C}_p}{j}$ of its subsets of cardinality j.

It is this way of using group actions to prove integrality results of this type which is fundamental for the proof of our theorems and which—first of all—suggested that a rather general variant of Witt's construction should exist, based on the equivariant combinatorics of arbitrary rather than of cyclic pro–finite groups, only.

References

CARTIER, P: *Groupes formels associées aux anneaux de Witt généralisées*, C.R.Acad.Sc.Paris, vol. **265** (1967), 49–52

CARTIER, P: *Quelques remarques sur la divisibilité des coefficients binomiaux*, L'Enseignement de Mathématique, vol. **16** (1970), 21–30

DRESS, A.W.M., SIEBENEICHER, Ch: *The Burnside Ring of profinite Groups and the Witt Vector Construction.*
Advances in Mathematics, vol. **70** (1988), 87–132.

DRESS A.W.M. AND SIEBENEICHER, Ch: *The Burnside Ring of the Infinite Cyclic Group and its Relations to the Necklace Algebra, λ–Rings and the Universal Ring of Witt Vectors*,
Advances in Mathematics, vol. **78** (1989), 1–41.

DRESS A.W.M. AND SIEBENEICHER, Ch: *A Multinomial Identity for Witt Vectors*, Advances in Mathematics, vol. **80** (1990), 250–260.

METROPOLIS N. AND ROTA G.–C.: *Witt Vectors and the Algebra of Necklaces*, Advances in Mathematics, vol. **50** (1983), 95–125.

WITT E.: *Zyklische Körper und Algebren der Charakteristik p vom Grade p^n*, J. Reine Angew. Math. (Crelle), vol. **176** (1937), 126-140.