Witt vectors. Part 1

Michiel Hazewinkel

Sidenotes by Darij Grinberg

Witt#1: The Burnside Theorem

[completed, not proofread]

Theorem 1, the Burnside theorem ([1], 19.10). Let G be a finite group, and let X and Y be finite G-sets. Then, the following two assertions $\mathcal{A}$ and $\mathcal{B}$ are equivalent:

Assertion $\mathcal{A}$: We have $X \cong Y$, where $\cong$ means isomorphism of G-sets.

Assertion $\mathcal{B}$: Every subgroup H of G satisfies $\left|X^H\right| = \left|Y^H\right|$.

Remark. Here and in the following, the sign $\cong$ means isomorphism of G-sets.

Remark on notation. Whenever G is a group, and U is a G-set, we use the following notations:

- If $u \in U$ is an element, then we let N_u denote the subgroup $\{g \in G \mid gu = u\}$ of G.
- If $u \in U$ is an element, then we let Gu denote the subset $\{gu \mid g \in G\}$ of U. Both Gu and $U \setminus Gu$ are G-sets (with the G-action inherited from U), and the G-set U is the disjoint union of these G-sets Gu and $U \setminus Gu$.
- If H is a subgroup of G, then we denote by U^H the subset $\{u \in U \mid Hu = \{u\}\} = \{u \in U \mid H \subseteq N_u\}$ of U (where Hu denotes the subset $\{hu \mid h \in H\}$ of U), and we denote by $U^{!H}$ the subset $\{u \in U \mid H = N_u\}$ of U. Obviously,

$$U^H = \{u \in U \mid H \subseteq N_u\} = \bigcup_{\substack{L \text{ subgroup of } G;\\ H \subseteq L}} \underbrace{\{u \in U \mid L = N_u\}}_{=U^{!L}} = \bigcup_{\substack{L \text{ subgroup of } G;\\ H \subseteq L}} U^{!L}.$$

Besides, the sets $U^{!L}$ for all subgroups L of G satisfying $H \subseteq L$ are pairwise disjoint (because for any two distinct subgroups L_1 and L_2 of G, the sets $U^{!L_1} = \{u \in U \mid L_1 = N_u\}$ and $U^{!L_2} = \{u \in U \mid L_2 = N_u\}$ are disjoint[1]). Thus,

$$\left|U^H\right| = \sum_{\substack{L \text{ subgroup of } G;\\ H \subseteq L}} \left|U^{!L}\right| = \left|U^{!H}\right| + \sum_{\substack{L \text{ subgroup of } G;\\ H \subseteq L;\ L \neq H}} \left|U^{!L}\right|. \tag{1}$$

Proof of Theorem 1. The implication $\mathcal{A} \Longrightarrow \mathcal{B}$ is completely obvious, so all it remains to verify is the implication $\mathcal{B} \Longrightarrow \mathcal{A}$. In other words, it remains to prove that if two finite G-sets X and Y are such that every subgroup H of G satisfies $\left|X^H\right| = \left|Y^H\right|$, then $X \cong Y$.

[1] since any element $u \in U^{!L_1} \cap U^{!L_2}$ would satisfy $L_1 = N_u$ and $L_2 = N_u$ in contradiction to $L_1 \neq L_2$

We will now prove this claim by strong induction over $|X|$. So, let X and Y be finite G-sets such that every subgroup H of G satisfies $\left|X^H\right| = \left|Y^H\right|$. We must show that $X \cong Y$. Our induction assumption states that

$$\begin{aligned}&\text{if } \widetilde{X} \text{ and } \widetilde{Y} \text{ are two finite } G\text{-sets such that } \left|\widetilde{X}\right| < |X| \text{ and such that}\\ &\text{every subgroup } H \text{ of } G \text{ satisfies } \left|\widetilde{X}^H\right| = \left|\widetilde{Y}^H\right|, \text{ then } \widetilde{X} = \widetilde{Y}. \end{aligned} \tag{2}$$

First, let us prove that

$$\left|X^{!H}\right| = \left|Y^{!H}\right| \qquad \text{for every subgroup } H \text{ of } G. \tag{3}$$

In fact, let us verify (3) by strong induction over $|G| - |H|$ (note that $|G| - |H|$ is always a nonnegative integer, since $H \subseteq G$). So we choose a subgroup H of G, and we want to prove that $\left|X^{!H}\right| = \left|Y^{!H}\right|$, assuming that

$$\left|X^{!L}\right| = \left|Y^{!L}\right| \text{ holds for every subgroup } L \text{ of } G \text{ which satisfies } |L| > |H|. \tag{4}$$

In fact, (1) yields

$$\left|X^H\right| = \left|X^{!H}\right| + \sum_{\substack{L \text{ subgroup of } G;\\ H \subseteq L;\ L \neq H}} \left|X^{!L}\right| \qquad \text{and} \qquad \left|Y^H\right| = \left|Y^{!H}\right| + \sum_{\substack{L \text{ subgroup of } G;\\ H \subseteq L;\ L \neq H}} \left|Y^{!L}\right|,$$

which yields $\left|X^{!H}\right| = \left|Y^{!H}\right|$, because $\sum\limits_{\substack{L \text{ subgroup of } G;\\ H \subseteq L;\ L \neq H}} \left|X^{!L}\right| = \sum\limits_{\substack{L \text{ subgroup of } G;\\ H \subseteq L;\ L \neq H}} \left|Y^{!L}\right|$ (since every subgroup L of G such that $H \subseteq L$ and $L \neq H$ must satisfy $|L| > |H|$, and thus $\left|X^{!L}\right| = \left|Y^{!L}\right|$ due to (4)) and $\left|X^H\right| = \left|Y^H\right|$. Hence, (3) is proven.

We will now prove that

$$\begin{aligned}&\text{for any two elements } x \in X \text{ and } y \in Y \text{ satisfying } N_x = N_y,\\ &\text{we have } Gx \cong Gy. \end{aligned} \tag{5}$$

In fact, define a map $f : Gx \to Gy$ as follows: For every element $\alpha \in Gx$, choose some $g \in G$ such that $\alpha = gx$, and define $f(\alpha)$ as gy. This definition is correct, because for every element $\alpha \in Gx$, there exists some $g \in G$ such that $\alpha = gx$ (by the definition of Gx), and even if different choices of $g \in G$ (for one fixed α) are possible, they all lead to one and the same value of gy (in fact, if two elements $g_1 \in G$ and $g_2 \in G$ both satisfy $\alpha = g_1 x$ and $\alpha = g_2 x$ for one and the same $\alpha \in Gx$, then $g_1 y = g_2 y$ [2]). Hence, for every element $\alpha \in Gx$ and *for every* $g \in G$ such that $\alpha = gx$, we have $f(\alpha) = gy$. In other words, we have $f(gx) = gy$ for every $g \in G$ (by applying the preceding sentence to $\alpha = gx$). This map f is a morphism of G-sets (since for every $\alpha \in Gx$ and every $h \in G$, we have $f(h\alpha) = hf(\alpha)$ [3]).

[2] In fact, $g_1 x = \alpha = g_2 x$ yields $g_2^{-1} g_1 x = x$, thus $g_2^{-1} g_1 \in N_x$, hence $g_2^{-1} g_1 \in N_y$ (since $N_x = N_y$) and thus $g_2^{-1} g_1 y = y$ and therefore $g_1 y = g_2 y$.

[3] In fact, let $g \in G$ be such that $\alpha = gx$ (such g exists, since $\alpha \in Gx$); then, the definition of f yields $f(\alpha) = gy$, and thus $f(h\alpha) = f(hgx) = h \underbrace{gy}_{=f(\alpha)} = hf(\alpha)$.

By interchanging x and y in the above, we can similarly define a map $f' : Gy \to Gx$ which satisfies $f'(gy) = gx$ for every $g \in G$ and which turns out to be a morphism of G-sets as well.

The two maps f and f' are mutually inverse (because $f' \circ f = \mathrm{id}_{Gx}$ [4] and similarly $f \circ f' = \mathrm{id}_{Gy}$). Hence, $f : Gx \to Gy$ is an isomorphism of G-sets. This proves (5).

Now, choose any $x \in X$ [5]. Then, $x \in \{u \in X \mid N_x = N_u\} = X^{!N_x}$. Thus, $X^{!N_x} \neq \varnothing$, so that $Y^{!N_x} \neq \varnothing$ (since $\left|X^{!N_x}\right| = \left|Y^{!N_x}\right|$ by (3)). So choose some $y \in Y^{!N_x}$. Then, $y \in Y^{!N_x} = \{u \in Y \mid N_x = N_u\}$, so that $N_x = N_y$. Hence, (5) yields that the G-sets Gx and Gy are isomorphic. Now, let us introduce the two G-sets $\widetilde{X} = X \setminus (Gx)$ and $\widetilde{Y} = Y \setminus (Gy)$. Clearly, $\left|\widetilde{X}\right| < |X|$. Besides, every subgroup H of G satisfies

$$\left|\widetilde{X}^H\right| = \left|\underbrace{(X \setminus (Gx))^H}_{= X^H \setminus (Gx)^H}\right| = \left|X^H \setminus (Gx)^H\right| = \left|X^H\right| - \left|(Gx)^H\right| \qquad \left(\text{since } (Gx)^H \subseteq X^H\right)$$

and similarly

$$\left|\widetilde{Y}^H\right| = \left|Y^H\right| - \left|(Gy)^H\right|$$

and thus $\left|\widetilde{X}^H\right| = \left|\widetilde{Y}^H\right|$ (because $\left|X^H\right| = \left|Y^H\right|$ by our assumption, and $\left|(Gx)^H\right| = \left|(Gy)^H\right|$ because of the isomorphy of the G-sets Gx and Gy). Hence, (2) yields $\widetilde{X} \cong \widetilde{Y}$. Now, the G-set X is the disjoint union of the G-sets Gx and $\widetilde{X}$ (since $\widetilde{X} = X \setminus (Gx)$), and the G-set Y is the disjoint union of the G-sets Gy and $\widetilde{Y}$ (since $\widetilde{Y} = Y \setminus (Gy)$). Hence, $Gx \cong Gy$ and $\widetilde{X} \cong \widetilde{Y}$ yield $X \cong Y$. This proves the implication $\mathcal{B} \Longrightarrow \mathcal{A}$, and thus, the proof of Theorem 1 is complete.

Remark: It is known that G-sets are, in a certain way, analogous to representations of the group G: Every G-set U canonically defines a permutation representation of G on the vector space k^G (the vector space of all functions from G to k) for every field k. Actually, it seems to me that G-sets can be considered as representations of G over the field $\mathbb{F}_1$, whatever this means. From this point of view, Theorem 1 appears as a kind of $\mathbb{F}_1$-analogue of the known fact that, over $\mathbb{C}$, any representation of a finite group is uniquely determined by its character. (Remember that the character of a representation over $\mathbb{C}$, evaluated at some element g of the group G, is the dimension of the invariant space of g. Over $\mathbb{C}$, the set $X^{\langle g \rangle}$ becomes a replacement for the invariant space of g. However, the analogy stops here because Theorem 1 needs all subgroups H and not just the cyclic ones. In fact, if we would replace "Every subgroup H" by "Every cyclic subgroup H" in Theorem 1, we would already have counterexamples for $G = (\mathbb{Z}/(2\mathbb{Z}))^2$.)

References

[1] Michiel Hazewinkel, *Witt vectors. Part 1*, revised version: 20 April 2008.

[4] In fact, for every $\alpha \in Gx$, there exists some $g \in G$ such that $\alpha = gx$ (by the definition of Gx), and thus

$$(f' \circ f)(\alpha) = f'(f(\alpha)) = f'\left(\underbrace{f(gx)}_{=gy}\right) = f'(gy) = gx = \alpha.$$

[5] If this is not possible (i. e., if $X = \varnothing$), then we are done anyway (since $X = \varnothing$ yields $|X| = 0$, thus $|Y| = 0$ since $|X| = \left|X^{\{1\}}\right| = \left|Y^{\{1\}}\right| = |Y|$ and therefore $Y = \varnothing$, yielding $X \cong Y$).