Witt vectors. Part 1

Michiel Hazewinkel
Sidenotes by Darij Grinberg

Witt#5c: The Chinese Remainder Theorem for Modules

[not completed, not proofread]

This is an auxiliary note; its goal is to prove a form of the Chinese Remainder Theorem that will be used in [2].

Definition 1. Let $\mathbb{P}$ denote the set of all primes. (A *prime* means an integer $n > 1$ such that the only divisors of n are n and 1. The word "divisor" means "positive divisor".)

Definition 2. We denote the set $\{0, 1, 2, ...\}$ by $\mathbb{N}$, and we denote the set $\{1, 2, 3, ...\}$ by $\mathbb{N}_+$. (Note that our notations conflict with the notations used by Hazewinkel in [1]; in fact, Hazewinkel uses the letter $\mathbb{N}$ for the set $\{1, 2, 3, ...\}$, which we denote by $\mathbb{N}_+$.)

Now, here is the Chinese Remainder Theorem in one of its most general forms:

Theorem 1. Let A be a commutative ring with unity. Let M be an A-module. Let $N \in \mathbb{N}$. Let I_1, I_2, ..., I_N be N ideals of A such that $I_i + I_j = A$ for any two elements i and j of $\{1, 2, ..., N\}$ satisfying $i < j$.

(a) Then, $I_1 I_2 ... I_N \cdot M = I_1 M \cap I_2 M \cap ... \cap I_N M$.

(b) Also, the map

$$\Phi : M \diagup (I_1 I_2 ... I_N \cdot M) \to \prod_{k=1}^{N} (M \diagup I_k M)$$

defined by

$$\Phi (m + I_1 I_2 ... I_N \cdot M) = (m + I_k M)_{k \in \{1,2,...,N\}} \qquad \text{for every } m \in M$$

is a well-defined isomorphism of A-modules.

(c) Let $(m_k)_{k \in \{1,2,...,N\}} \in M^N$ be a family of elements of M. Then, there exists an element m of M such that

$$(m_k \equiv m \operatorname{mod} I_k M \text{ for every } k \in \{1, 2, ..., N\}) . \qquad (1)$$

Proof of Theorem 1. **(a)** Theorem 1 **(a)** occurred as Theorem 1 in [1], and we won't repeat the proof given there.

(b) Let us first forget the definition of Φ made in Theorem 1 **(b)** (until we have shown that it is indeed well-defined).

For any integers $i \in \{1, 2, ..., N\}$ and $j \in \{1, 2, ..., N\}$ satisfying $i < j$, we can find an element $a_{i,j}$ of I_i and an element $a_{j,i}$ of I_j such that $a_{i,j} + a_{j,i} = 1$ (since

$1 \in A = I_i + I_j$). Fix such elements $a_{i,j}$ and $a_{j,i}$ for all pairs of integers $i \in \{1, 2, ..., N\}$ and $j \in \{1, 2, ..., N\}$ satisfying $i < j$. Then,

$$\left(\begin{array}{c} a_{i,j} \in I_i, \ a_{j,i} \in I_j \text{ and } a_{i,j} + a_{j,i} = 1 \text{ for any} \\ \text{integers } i \in \{1, 2, ..., N\} \text{ and } j \in \{1, 2, ..., N\} \text{ satisfying } i < j \end{array} \right). \quad (2)$$

Consequently, we have

$$\left(\begin{array}{c} a_{i,j} \in I_i, \ a_{j,i} \in I_j \text{ and } a_{i,j} + a_{j,i} = 1 \text{ for any} \\ \text{integers } i \in \{1, 2, ..., N\} \text{ and } j \in \{1, 2, ..., N\} \text{ satisfying } i \neq j \end{array} \right) \quad (3)$$

[1]. Notice that

$$\prod_{\substack{i \in \{1,2,...,N\};\\ i \neq \ell}} a_{i,\ell} \in I_k \text{ for any } \ell \in \{1, 2, ..., N\} \text{ and } k \in \{1, 2, ..., N\} \text{ satisfying } \ell \neq k. \quad (4)$$

[2] Also,

$$\prod_{\substack{i \in \{1,2,...,N\};\\ i \neq k}} a_{i,k} \in 1 + I_k \qquad \text{for every } k \in \{1, 2, ..., N\}. \quad (5)$$

[3]

Now, define a map

$$\varphi : M \to \prod_{k=1}^{N} (M \diagup I_k M) \qquad \text{by}$$
$$\varphi(m) = (m + I_k M)_{k \in \{1,2,...,N\}} \qquad \text{for every } m \in M.$$

Clearly, φ is a homomorphism of A-modules. We have $I_1 I_2 ... I_N \cdot M \subseteq \operatorname{Ker} \varphi$ (since

[1] *Proof of (3):* Let $i \in \{1, 2, ..., N\}$ and $j \in \{1, 2, ..., N\}$ be two integers satisfying $i \neq j$. Since $i \neq j$, we must have either $i < j$ and $i > j$. But in both of these cases, (3) can be derived from (2) (in fact, if $i < j$, then (3) directly follows from (2), and if $i > j$, then (3) follows from (2) (applied to j and i instead of i and j)). Hence, (3) is proven.

[2] *Proof of (4):* Let $\ell \in \{1, 2, ..., N\}$ and $k \in \{1, 2, ..., N\}$ satisfy $\ell \neq k$. Then, (3) (applied to $i = k$ and $j = \ell$) yields $a_{k,\ell} \in I_k$, $a_{\ell,k} \in I_\ell$ and $a_{k,\ell} + a_{\ell,k} = 1$. But the product $\prod\limits_{\substack{i \in \{1,2,...,N\};\\ i \neq \ell}} a_{i,\ell}$ contains the factor $a_{k,\ell}$ (because $k \neq \ell$), and thus lies in I_k (since $a_{k,\ell} \in I_k$, and since I_k is an ideal of A). This proves (4).

[3] *Proof of (5):* Let $k \in \{1, 2, ..., N\}$. Applying (3) to $j = k$, we obtain the following:

$$a_{i,k} \in I_i, \ a_{k,i} \in I_k \text{ and } a_{i,k} + a_{k,i} = 1 \text{ for any integer } i \in \{1, 2, ..., N\} \text{ satisfying } i \neq k.$$

Thus, for any integer $i \in \{1, 2, ..., N\}$ satisying $i \neq k$, we have $1 = a_{i,k} + \underbrace{a_{k,i}}_{\substack{\equiv 0 \bmod I_k \\ (\text{since } a_{k,i} \in I_k)}} \equiv a_{i,k} \bmod I_k$.

Hence, $\prod\limits_{\substack{i \in \{1,2,...,N\};\\ i \neq k}} 1 \equiv \prod\limits_{\substack{i \in \{1,2,...,N\};\\ i \neq k}} a_{i,k} \bmod I_k$. In other words, $\prod\limits_{\substack{i \in \{1,2,...,N\};\\ i \neq k}} a_{i,k} \equiv \prod\limits_{\substack{i \in \{1,2,...,N\};\\ i \neq k}} 1 = 1 \bmod I_k$, so that $\prod\limits_{\substack{i \in \{1,2,...,N\};\\ i \neq k}} a_{i,k} \in 1 + I_k$. This proves (5).

every $m \in I_1 I_2 ... I_N \cdot M$ satisfies

$$\varphi(m) = \left(\underbrace{m + I_k M}_{\substack{= I_k M \text{ (since} \\ m \in I_1 I_2 ... I_N \cdot M \subseteq I_k M)}} \right)_{k \in \{1,2,...,N\}} = \left(\underbrace{I_k M}_{\substack{\text{this is the zero} \\ \text{of the } A\text{-module} \\ M / I_k M}} \right)_{k \in \{1,2,...,N\}} = (0)_{k \in \{1,2,...,N\}} = 0$$

and thus $m \in \operatorname{Ker} \varphi$). Hence, φ induces a homomorphism

$$\Phi : M / (I_1 I_2 ... I_N \cdot M) \to \prod_{k=1}^{N} (M / I_k M)$$

of A-modules satisfying

$$\Phi(m + I_1 I_2 ... I_N \cdot M) = (m + I_k M)_{k \in \{1,2,...,N\}} \qquad \text{for every } m \in M.$$

This proves that the map Φ of Theorem 1 **(b)** is well-defined and a homomorphism of A-modules. We have yet to show that this Φ is an isomorphism.

Define a map

$$\Psi : \prod_{k=1}^{N} (M / I_k M) \to M / (I_1 I_2 ... I_N \cdot M)$$

by

$$\Psi\left((m_k + I_k M)_{k \in \{1,2,...,N\}} \right) = \sum_{\ell=1}^{N} \left(\prod_{\substack{i \in \{1,2,...,N\}; \\ i \neq \ell}} a_{i,\ell} \right) m_\ell + I_1 I_2 ... I_N \cdot M$$
$$\text{for every } (m_k)_{k \in \{1,2,...,N\}} \in M^N.$$

This map Ψ is indeed well-defined, since the residue class $\sum\limits_{\ell=1}^{N} \left(\prod\limits_{\substack{i \in \{1,2,...,N\}; \\ i \neq \ell}} a_{i,\ell} \right) m_\ell + I_1 I_2 ... I_N \cdot M$ depends only on $(m_k + I_k M)_{k \in \{1,2,...,N\}}$ and not on $(m_k)_{k \in \{1,2,...,N\}}$ (because if $(m_k)_{k \in \{1,2,...,N\}} \in M^N$ and $(m'_k)_{k \in \{1,2,...,N\}} \in M^N$ are two families satisfying $(m_k + I_k M)_{k \in \{1,2,...,N\}} = (m'_k + I_k M)_{k \in \{1,2,...,N\}}$ in $\prod\limits_{k=1}^{N} (M / I_k M)$, then

$$\sum_{\ell=1}^{N} \left(\prod_{\substack{i \in \{1,2,...,N\}; \\ i \neq \ell}} a_{i,\ell} \right) m_\ell + I_1 I_2 ... I_N \cdot M = \sum_{\ell=1}^{N} \left(\prod_{\substack{i \in \{1,2,...,N\}; \\ i \neq \ell}} a_{i,\ell} \right) m'_\ell + I_1 I_2 ... I_N \cdot M$$

[4]).

[4] *Proof.* In fact, $(m_k + I_k M)_{k \in \{1,2,...,N\}} = (m'_k + I_k M)_{k \in \{1,2,...,N\}}$ yields $m_k + I_k M = m'_k + I_k M$

Every family $(m_k)_{k\in\{1,2,...,N\}} \in M^N$ satisfies

$$(\Phi \circ \Psi)\left((m_k + I_k M)_{k\in\{1,2,...,N\}}\right) = \Phi\left(\Psi\left((m_k + I_k M)_{k\in\{1,2,...,N\}}\right)\right)$$
$$= \Phi\left(\sum_{\ell=1}^{N}\left(\prod_{\substack{i\in\{1,2,...,N\};\\ i\neq\ell}} a_{i,\ell}\right) m_\ell + I_1 I_2 ... I_N \cdot M\right)$$
$$\left(\text{by the definition of } \Psi\left((m_k + I_k M)_{k\in\{1,2,...,N\}}\right)\right)$$
$$= \left(\sum_{\ell=1}^{N}\left(\prod_{\substack{i\in\{1,2,...,N\};\\ i\neq\ell}} a_{i,\ell}\right) m_\ell + I_k M\right)_{k\in\{1,2,...,N\}} \qquad (6)$$
$$(\text{by the definition of } \Phi).$$

---

for each $k \in \{1, 2, ..., N\}$, and thus $m_k - m'_k \in I_k M$ for each $k \in \{1, 2, ..., N\}$. In other words, $m_\ell - m'_\ell \in I_\ell M$ for each $\ell \in \{1, 2, ..., N\}$. Now,

$$\sum_{\ell=1}^{N}\left(\prod_{\substack{i\in\{1,2,...,N\};\\ i\neq\ell}} a_{i,\ell}\right) m_\ell - \sum_{\ell=1}^{N}\left(\prod_{\substack{i\in\{1,2,...,N\};\\ i\neq\ell}} a_{i,\ell}\right) m'_\ell$$
$$= \sum_{\ell=1}^{N}\left(\prod_{\substack{i\in\{1,2,...,N\};\\ i\neq\ell}} \underbrace{a_{i,\ell}}_{\in I_i}\right) \underbrace{(m_\ell - m'_\ell)}_{\in I_\ell M} \in \sum_{\ell=1}^{N} \underbrace{\left(\prod_{\substack{i\in\{1,2,...,N\};\\ i\neq\ell}} I_i\right) I_\ell}_{=\prod_{i\in\{1,2,...,N\}} I_i = I_1 I_2 ... I_N} M = \sum_{\ell=1}^{N} I_1 I_2 ... I_N \cdot M$$
$$\subseteq I_1 I_2 ... I_N \cdot M \qquad (\text{since } I_1 I_2 ... I_N \cdot M \text{ is an } A\text{-module}),$$

so that

$$\sum_{\ell=1}^{N}\left(\prod_{\substack{i\in\{1,2,...,N\};\\ i\neq\ell}} a_{i,\ell}\right) m_\ell + I_1 I_2 ... I_N \cdot M = \sum_{\ell=1}^{N}\left(\prod_{\substack{i\in\{1,2,...,N\};\\ i\neq\ell}} a_{i,\ell}\right) m'_\ell + I_1 I_2 ... I_N \cdot M,$$

qed.

Since every $k \in \{1, 2, ..., N\}$ satisfies

$$\begin{aligned}
&\underbrace{\sum_{\ell=1}^{N}}_{=\sum_{\ell\in\{1,2,...,N\}}} \left(\prod_{\substack{i\in\{1,2,...,N\};\\ i\neq\ell}} a_{i,\ell} \right) m_\ell \\
&= \sum_{\ell\in\{1,2,...,N\}} \left(\prod_{\substack{i\in\{1,2,...,N\};\\ i\neq\ell}} a_{i,\ell} \right) m_\ell \\
&= \sum_{\substack{\ell\in\{1,2,...,N\};\\ \ell\neq k}} \underbrace{\left(\prod_{\substack{i\in\{1,2,...,N\};\\ i\neq\ell}} a_{i,\ell} \right)}_{\substack{\in I_k \\ \text{(by (4))}}} m_\ell + \underbrace{\sum_{\substack{\ell\in\{1,2,...,N\};\\ \ell=k}} \left(\prod_{\substack{i\in\{1,2,...,N\};\\ i\neq\ell}} a_{i,\ell} \right) m_\ell}_{=\left(\prod_{\substack{i\in\{1,2,...,N\};\\ i\neq k}} a_{i,k} \right) m_k} \\
&\in \sum_{\substack{\ell\in\{1,2,...,N\};\\ \ell\neq k}} I_k m_\ell + \underbrace{\left(\prod_{\substack{i\in\{1,2,...,N\};\\ i\neq k}} a_{i,k} \right)}_{\substack{\in 1+I_k \\ \text{(by (5))}}} m_k \\
&\subseteq \sum_{\substack{\ell\in\{1,2,...,N\};\\ \ell\neq k}} I_k m_\ell + \underbrace{(1 + I_k)\, m_k}_{=m_k + I_k m_k} = \sum_{\substack{\ell\in\{1,2,...,N\};\\ \ell\neq k}} \underbrace{I_k m_\ell}_{\subseteq I_k M} + m_k + \underbrace{I_k m_k}_{\subseteq I_k M} \\
&\subseteq I_k M + m_k + I_k M = \underbrace{I_k M + I_k M}_{=I_k M \text{ (since } I_k M \text{ is an } A\text{-module)}} + m_k = m_k + I_k M
\end{aligned}$$

and thus

$$\sum_{\ell=1}^{N} \left(\prod_{\substack{i\in\{1,2,...,N\};\\ i\neq\ell}} a_{i,\ell} \right) m_\ell + I_k M = m_k + I_k M,$$

the equation (6) becomes

$$\begin{aligned}
(\Phi \circ \Psi)\left((m_k + I_k M)_{k\in\{1,2,...,N\}} \right) &= \left(\underbrace{\sum_{\ell=1}^{N} \left(\prod_{\substack{i\in\{1,2,...,N\};\\ i\neq\ell}} a_{i,\ell} \right) m_\ell + I_k M}_{=m_k + I_k M} \right)_{k\in\{1,2,...,N\}} \\
&= (m_k + I_k M)_{k\in\{1,2,...,N\}} .
\end{aligned}$$

Since this holds for every $(m_k)_{k\in\{1,2,...,N\}} \in M^N$, this yields $\Phi \circ \Psi = \text{id}$ (because every element of $\prod_{k=1}^{N} (M / I_k M)$ can be written in the form $(m_k + I_k M)_{k\in\{1,2,...,N\}}$ for some $(m_k)_{k\in\{1,2,...,N\}} \in M^N$).

Now we are going to prove that the A-module homomorphism Φ is injective. In fact, let $m \in M$ be such that $\Phi(m + I_1 I_2 ... I_N \cdot M) = 0$. Then,

$$0 = \Phi(m + I_1 I_2 ... I_N \cdot M) = (m + I_k M)_{k\in\{1,2,...,N\}},$$

so that $0 = m + I_k M$ in $M / I_k M$ for every $k \in \{1, 2, ..., N\}$. This yields $m \in I_k M$ for every $k \in \{1, 2, ..., N\}$ (because $0 = m + I_k M$ rewrites as $m \in I_k M$), and thus $m \in I_1 M \cap I_2 M \cap ... \cap I_N M$. Using Theorem 1 **(a)**, this rewrites as $m \in I_1 I_2 ... I_N \cdot M$.

Thus, we have proven that

$$\text{every } m \in M \text{ such that } \Phi(m + I_1 I_2 ... I_N \cdot M) = 0 \text{ must satisfy } m \in I_1 I_2 ... I_N \cdot M. \quad (7)$$

Now, if $\alpha \in M / (I_1 I_2 ... I_N \cdot M)$ satisfies $\Phi(\alpha) = 0$, then $\alpha = 0$. [5] Thus, the homomorphism Φ is injective. Consequently, Φ is left cancellable, so that $\Phi \circ (\Psi \circ \Phi) = \underbrace{\Phi \circ \Psi}_{=\text{id}} \circ \Phi = \Phi = \Phi \circ \text{id}$ yields $\Psi \circ \Phi = \text{id}$.

Since $\Phi \circ \Psi = \text{id}$ and $\Psi \circ \Phi = \text{id}$, the map Ψ must be an inverse map of the map Φ. Hence, Φ is bijective. Since Φ is an A-module homomorphism, this yields that Φ is an A-module isomorphism, and thus Theorem 1 **(b)** is proven.

(c) Let

$$\alpha = \Phi^{-1}\left((m_k + I_k M)_{k\in\{1,2,...,N\}}\right)$$

(where Φ^{-1} is a well-defined map, since Φ is an isomorphism). Then, $\alpha \in M / (I_1 I_2 ... I_N \cdot M)$, and therefore $\alpha = m + I_1 I_2 ... I_N \cdot M$ for some $m \in M$. Consequently,

$$\Phi^{-1}\left((m_k + I_k M)_{k\in\{1,2,...,N\}}\right) = \alpha = m + I_1 I_2 ... I_N \cdot M,$$

so that

$$(m_k + I_k M)_{k\in\{1,2,...,N\}} = \Phi(m + I_1 I_2 ... I_N \cdot M) = (m + I_k M)_{k\in\{1,2,...,N\}}$$

(by the definition of Φ). Hence, we have $m_k + I_k M = m + I_k M$ for every $k \in \{1, 2, ..., N\}$. This yields (1) (since $m_k + I_k M = m + I_k M$ is equivalent to $m_k \equiv m \bmod I_k M$). Thus, Theorem 1 **(c)** is proven.

Here is a trivial corollary of Theorem 1 which is used in [2]:

> **Corollary 2.** Let M be an Abelian group (written additively). Let P be a finite set of positive integers such that any two distinct elements of P are coprime. Let $(c_p)_{p\in P} \in M^P$ be a family of elements of M. Then, there exists an element m of M such that
>
> $$(c_p \equiv m \bmod pM \text{ for every } p \in P).$$

[5] In fact, we can find some $m \in M$ such that $\alpha = m + I_1 I_2 ... I_N \cdot M$ (by the definition of the factor module $M / (I_1 I_2 ... I_N \cdot M)$), and thus $\Phi(\alpha) = 0$ becomes $\Phi(m + I_1 I_2 ... I_N \cdot M) = 0$, so that (7) yields $m \in I_1 I_2 ... I_N \cdot M$. In other words, $m + I_1 I_2 ... I_N \cdot M = 0$ in $M / (I_1 I_2 ... I_N \cdot M)$. Since $\alpha = m + I_1 I_2 ... I_N \cdot M$, this rewrites as $\alpha = 0$, qed.

Proof of Corollary 2. Since P is a finite set of positive integers, it can be written in the form $P = \{p_1, p_2, ..., p_N\}$, where p_1, p_2, ..., p_N are pairwise distinct positive integers and $N = |P|$. Define a family $(m_k)_{k\in\{1,2,...,N\}} \in M^N$ of elements of M by $m_k = c_{p_k}$ for every $k \in \{1, 2, ..., N\}$.

Now, let A be the ring $\mathbb{Z}$. Then, M is a $\mathbb{Z}$-module. For every $k \in \{1, 2, ..., N\}$, define an ideal I_k of $\mathbb{Z}$ by $I_k = p_k\mathbb{Z}$. Then, for any two elements i and j of $\{1, 2, ..., N\}$ satisfying $i < j$, we have $I_i + I_j = A$ [6]. Hence, Theorem 1 **(c)** yields that there exists an element m of M such that

$$(m_k \equiv m \operatorname{mod} I_k M \text{ for every } k \in \{1, 2, ..., N\}) . \tag{8}$$

Hence, $c_p \equiv m \operatorname{mod} pM$ for every $p \in P$ [7]. This proves Corollary 2.

A yet more trivial consequence of Corollary 2:

Corollary 3. Let M be an Abelian group (written additively). Let $P \subseteq \mathbb{P}$ be a finite set of primes. Let $(c_p)_{p\in P} \in M^P$ be a family of elements of M. Then, there exists an element m of M such that

$$(c_p \equiv m \operatorname{mod} pM \text{ for every } p \in P) .$$

Proof of Corollary 3. Corollary 3 directly follows from Corollary 2, because any two distinct elements of P are coprime (in fact, any two distinct elements of P are two distinct primes, and two distinct primes are always coprime).

References

[1] Darij Grinberg, *Witt#5: Around the integrality criterion 9.93.*
http://www.cip.ifi.lmu.de/~grinberg/algebra/witt5.pdf

[2] Darij Grinberg, *Witt#5b: Some divisibilities for big Witt polynomials.*
http://www.cip.ifi.lmu.de/~grinberg/algebra/witt5b.pdf

[6] In fact, let i and j be two elements of $\{1, 2, ..., N\}$ satisfying $i < j$. Then, p_i and p_j are distinct elements of P (since $i < j$ yields $i \neq j$, and since p_1, p_2, ..., p_N are pairwise distinct). Hence, p_i and p_j are coprime (because any two distinct elements of P are coprime). Thus, Bezout's Theorem yields that there exist $u \in \mathbb{Z}$ and $v \in \mathbb{Z}$ satisfying $p_i u + p_j v = 1$. Hence, $1 = \underbrace{p_i u}_{\in p_i\mathbb{Z} = I_i} + \underbrace{p_j v}_{\in p_j\mathbb{Z} = I_j} \in I_i + I_j$ and thus $I_i + I_j = \mathbb{Z} = A$.

[7] *Proof.* Let $p \in P$. Then, there exists $k \in \{1, 2, ..., N\}$ such that $p = p_k$ (since $P = \{p_1, p_2, ..., p_N\}$). Hence, (8) yields $m_k \equiv m \operatorname{mod} I_k M$. Since $m_k = c_{p_k} = c_p$ and $I_k M = p_k\mathbb{Z} \cdot M = p_k M = pM$, this rewrites as $c_p \equiv m \operatorname{mod} pM$, qed.