Definition. Let $R$ be a commutative ring with unity. Let $n$ be a positive integer. Let $M$ be an $R$-module. If $m_1, m_2, \ldots, m_n$ are $n$ elements of $M$, then we define an $R$-submodule $\langle m_1, m_2, \ldots, m_n \rangle_R$ of $M$ by

$$\langle m_1, m_2, \ldots, m_n \rangle_R = \left\{ \sum_{j=1}^{n} r_j m_j \mid (r_1, r_2, \ldots, r_n) \in R^n \right\}.$$  

(This $R$-submodule $\langle m_1, m_2, \ldots, m_n \rangle_R$ is known as the $R$-submodule of $M$ generated by the elements $m_1, m_2, \ldots, m_n$.)

Problem. Let $R$ be a commutative ring with unity. Let $n \in \mathbb{N}$. Let $a_1, a_2, \ldots, a_n$ be $n$ elements of $R$, and let $b_1, b_2, \ldots, b_n$ be $n$ elements of $R$. Assume that

$$b_i b_j = 0 \text{ for any } i \in \{1, 2, \ldots, n\} \text{ and any } j \in \{1, 2, \ldots, n\} \text{ satisfying } i < j.$$  

(1)

Also, assume that $\sum_{k=1}^{n} a_k b_k = 1$.

Let $T$ be a free $R$-module of rank $n$. Let $(e_1, e_2, \ldots, e_n)$ be a basis of this free $R$-module $T$.

Prove that the $R$-module $T \setminus \langle b_1 e_1, b_2 e_2, \ldots, b_n e_n \rangle_R$ is a free $R$-module of rank $n-1$.

Solution by Darij Grinberg.

First, notice that

$$b_u b_v = 0 \text{ for any } u \in \{1, 2, \ldots, n\} \text{ and any } v \in \{1, 2, \ldots, n\} \text{ satisfying } u \neq v.$$  

(2)

[Proof of (2). For any $u \in \{1, 2, \ldots, n\}$ and any $v \in \{1, 2, \ldots, n\}$ satisfying $u \neq v$, we must have either $u < v$ or $v < u$. In both of these cases, $b_u b_v = 0$ holds \footnote{In fact,}

$\bullet$ if $u < v$, then $b_u b_v = 0$ (by (1), applied to $i = u$ and $j = v$);

$\bullet$ if $v < u$, then $b_u b_v = b_v b_u = 0$ (since $b_v b_u = 0$ (by (1), applied to $i = v$ and $j = u$)).]  

Furthermore, we notice that

$$a_u b_u^2 = b_u \text{ for any } u \in \{1, 2, \ldots, n\}.$$  

(3)
Let \( u \in \{1, 2, \ldots, n\} \). Then,
\[
\sum_{v \in \{1, 2, \ldots, n\}} a_v b_v = \sum_{v=1}^{n} a_v b_v = \sum_{k=1}^{n} a_k b_k
\]
\[
= \sum_{v=1}^{n}
\]
(here we renamed the summation index \( v \) as \( k \))
\[
= 1
\]
and thus
\[
b_u \cdot \sum_{v \in \{1, 2, \ldots, n\}} a_v b_v = b_u \cdot 1 = b_u.
\]

Compared with
\[
b_u \cdot \sum_{v \in \{1, 2, \ldots, n\}} a_v b_v = \sum_{v \in \{1, 2, \ldots, n\}} a_v b_u b_v
\]
\[
= \sum_{v \in \{1, 2, \ldots, n\}; v \neq u} a_v \underbrace{b_u b_v}_{= 0 \text{ (by 2)}} + \sum_{v \in \{1, 2, \ldots, n\}; v = u} a_v b_u b_v
\]
\[
= \sum_{v \in \{1, 2, \ldots, n\}; v \neq u} a_v \cdot 0 + a_u \underbrace{b_u b_u}_{= b_u^2} = a_u b_u^2.
\]
\[
= 0
\]
this yields \( a_u b_u^2 = b_u \). Thus, \([3]\) is proven.

For every vector \( w \in T \), we denote by \( \overline{w} \) the element \( w + \langle b_1 e_1, b_2 e_2, \ldots, b_n e_n \rangle_R \) of \( T / \langle b_1 e_1, b_2 e_2, \ldots, b_n e_n \rangle_R \). (In other words, for every vector \( w \in T \), we denote by \( \overline{w} \) the equivalence class of \( w \) modulo the submodule \( \langle b_1 e_1, b_2 e_2, \ldots, b_n e_n \rangle_R \).)

For every \( k \in \{1, 2, \ldots, n-1\} \), define an element \( s_k \) of \( T / \langle b_1 e_1, b_2 e_2, \ldots, b_n e_n \rangle_R \) by
\[
s_k = \sum_{(i, j) \in \{1, 2, \ldots, n\}^2} a_i b_i \overline{e_j};
\]
\[
j - i = k \mod n
\]
We are now going to prove two lemmata:

**Assertion 1:** Let \( (t_1, t_2, \ldots, t_{n-1}) \in R^{n-1} \). If \( \sum_{k=1}^{n-1} t_k s_k = 0 \), then \( (t_1, t_2, \ldots, t_{n-1}) = 0 \) (where \( 0 \) denotes the zero vector \( \left( 0, 0, \ldots, 0 \right) \in R^{n-1} \)).

**Assertion 2:** We have \( \langle s_1, s_2, \ldots, s_{n-1} \rangle_R = T / \langle b_1 e_1, b_2 e_2, \ldots, b_n e_n \rangle_R \).
Proof of Assertion 1. Assume that $\sum_{k=1}^{n-1} t_k s_k = 0$. Then,

$$0 = \sum_{k=1}^{n-1} t_k \sum_{j=1}^{n} s_j = \sum_{k \in \{1,2,\ldots,n-1\}} t_k \sum_{j=1}^{n} a_i b_j e_j$$

$$= \sum_{k \in \{1,2,\ldots,n-1\}} \sum_{j \equiv k \mod n} t_k a_i b_j e_j$$

so that

$$\sum_{j=1}^{n} \sum_{k \in \{1,2,\ldots,n-1\}} t_k a_i b_j e_j \in \langle b_1 e_1, b_2 e_2, \ldots, b_n e_n \rangle_R$$

$$= \left\{ \sum_{j=1}^{n} r_j b_j e_j \mid (r_1, r_2, \ldots, r_n) \in \mathbb{R}^n \right\}$$

(by the definition of $\langle b_1 e_1, b_2 e_2, \ldots, b_n e_n \rangle_R$). In other words, there exists some $(r_1, r_2, \ldots, r_n) \in \mathbb{R}^n$ such that

$$\sum_{j=1}^{n} \sum_{k \in \{1,2,\ldots,n-1\}} t_k a_i b_j e_j = \sum_{j=1}^{n} r_j b_j e_j.$$

Consider this $(r_1, r_2, \ldots, r_n)$. Then,

$$\sum_{j=1}^{n} \left( \sum_{i \in \{1,2,\ldots,n\}} \sum_{k \in \{1,2,\ldots,n-1\}} t_k a_i b_i - r_j b_j \right) e_j$$

$$= \sum_{j=1}^{n} \sum_{i \in \{1,2,\ldots,n\}} \sum_{k \in \{1,2,\ldots,n-1\}} t_k a_i b_i e_j - \sum_{j=1}^{n} r_j b_j e_j$$

$$= \sum_{j=1}^{n} \sum_{k \in \{1,2,\ldots,n-1\}} \sum_{j \equiv k \mod n} t_k a_i b_i e_j - \sum_{j=1}^{n} r_j b_j e_j - \sum_{j=1}^{n} r_j b_j e_j = 0.$$
Since the vectors $e_1, e_2, \ldots, e_n$ are linearly independent (since $(e_1, e_2, \ldots, e_n)$ is a basis of the $R$-module $T$), this yields
\[
\sum_{i \in \{1, 2, \ldots, n\}} \sum_{k \in \{1, 2, \ldots, n-1\}; \ j \equiv k \mod n} t_k a_i b_i - r_j b_j = 0 \quad \text{for every } j \in \{1, 2, \ldots, n\}.
\]

\[2\] In other words,
\[
\sum_{i \in \{1, 2, \ldots, n\}} \sum_{k \in \{1, 2, \ldots, n-1\}; \ j \equiv k \mod n} t_k a_i b_i = r_j b_j \quad \text{for every } j \in \{1, 2, \ldots, n\}.
\]

Next, we are going to show that $t_k b_\ell = 0$ for any $\lambda \in \{1, 2, \ldots, n-1\}$ and any $\ell \in \{1, 2, \ldots, n\}$.

**Proof of (5).** Let $\lambda \in \{1, 2, \ldots, n-1\}$ and $\ell \in \{1, 2, \ldots, n\}$. Let $\phi$ be the remainder of $\lambda + \ell - 1$ upon division by $n$. Then, $\phi \in \{0, 1, \ldots, n-1\}$ and $\phi \equiv \lambda + \ell - 1 \mod n$.

Let $j = \phi + 1$. Then, $j = \phi + 1 \in \{1, 2, \ldots, n\}$ (since $\phi \in \{0, 1, \ldots, n-1\}$).

Also, $j \equiv \lambda + \ell \mod n$ (since $j = \phi + 1 \equiv \lambda + \ell - 1 \mod n$).

Let $a_i = 0$ for every $i \in \{1, 2, \ldots, n\}$. Applying this to $a_j = \sum_{i \in \{1, 2, \ldots, n\}} \sum_{k \in \{1, 2, \ldots, n-1\}; \ j \equiv k \mod n} t_k a_i b_i - r_j b_j$, we obtain
\[
\left(\sum_{i \in \{1, 2, \ldots, n\}} \sum_{k \in \{1, 2, \ldots, n-1\}; \ j \equiv k \mod n} t_k a_i b_i - r_j b_j \right) e_j = 0,
\]

thus $j - \ell \equiv k \mod n$. Then, $k \equiv j - \ell \equiv \lambda \mod n$, so that $n \nmid \lambda - k$. Thus,
\[
\lambda - k \in \mathbb{Z}.
\]

But we have $\lambda \in \{1, 2, \ldots, n-1\}$ and thus $0 < \lambda < n$. Also, $k \in \{1, 2, \ldots, n-1\}$ and

**Proof of (6):** Let $k \in \{1, 2, \ldots, n-1\}$.

Assume that $j - \ell \equiv k \mod n$. Then, $k \equiv j - \ell \equiv \lambda \mod n$, so that $n \nmid \lambda - k$. Thus,

$\lambda - k \in \mathbb{Z}$. 

Hence, (3) (applied to $u = j$ and $\lambda \equiv 0 \mod n$)

**Proof.** The vectors $e_1, e_2, \ldots, e_n$ are linearly independent. Hence, if $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in R^n$ is an $n$-tuple satisfying $\sum_{j=1}^{n} \alpha_j e_j = 0$, then we have $(\alpha_j = 0$ for every $j \in \{1, 2, \ldots, n\}$). Applying this to $\alpha_j = \sum_{i \in \{1, 2, \ldots, n\}} \sum_{k \in \{1, 2, \ldots, n-1\}; \ j \equiv k \mod n} t_k a_i b_i - r_j b_j$, we obtain
\[
\left(\sum_{i \in \{1, 2, \ldots, n\}} \sum_{k \in \{1, 2, \ldots, n-1\}; \ j \equiv k \mod n} t_k a_i b_i - r_j b_j \right) e_j = 0,
\]

thus $\lambda \equiv 0 \mod n$. Hence, (2) (applied to $u = j$ and $\lambda \equiv 0 \mod n$)

$\lambda \equiv j - \ell \equiv k \mod n$. Then, $k \equiv j - \ell \equiv \lambda \mod n$, so that $n \nmid \lambda - k$. Thus,

$\lambda - k \in \mathbb{Z}$.
\( v = \ell \) shows that \( b_j b_\ell = 0 \). Now,

\[
\sum_{i \in \{1, 2, \ldots, n\}} \sum_{k \in \{1, 2, \ldots, n-1\}; j - i \equiv k \mod n} t_k a_i b_i b_\ell = r_j b_j b_\ell = r_j \cdot 0 = 0.
\]

thus \( 0 < k < n \). Combining

\[
\frac{\lambda - k}{n} > \frac{0 - n}{n} = -1
\]

(since \( \lambda > 0 \) and \( k < n \))

and

\[
\frac{\lambda - k}{n} < \frac{n - 0}{n} = 1,
\]

(since \( \lambda < n \) and \( k > 0 \))

we obtain \( \frac{\lambda - k}{n} \in [0, 1] \). This (combined with \( \frac{\lambda - k}{n} \in \mathbb{Z} \)) yields \( \frac{\lambda - k}{n} \in \mathbb{Z} \cap [0, 1] = \{0\}. \)

Hence, \( \frac{\lambda - k}{n} = 0 \), so that \( \lambda - k = 0 \), and thus \( k = \lambda \).

Now, let us forget that we assumed that \( j - \ell \equiv k \mod n \). We thus have proven that \( k = \lambda \) if \( j - \ell \equiv k \mod n \). In other words, we have proven the implication

\[
(j - \ell \equiv k \mod n) \implies (k = \lambda). \tag{7}
\]

But the implication

\[
(k = \lambda) \implies (j - \ell \equiv k \mod n) \tag{8}
\]

also holds (because if \( k = \lambda \), then \( j - \ell \equiv \lambda = k \mod n \)). Combining the implications \( \tag{7} \) and \( \tag{8} \), we obtain the logical equivalence

\[
(j - \ell \equiv k \mod n) \iff (k = \lambda).
\]

In other words, the assertions \( j - \ell \equiv k \mod n \) and \( k = \lambda \) are equivalent. This proves \( \tag{6} \).
But on the other hand,

\[ \sum_{i \in \{1,2,\ldots,n\}} \sum_{k \in \{1,2,\ldots,n-1\}} \sum_{j = i \mod n} t_k a_i b_j b_{\ell} \]

\[ = \sum_{i = \ell} \sum_{k \in \{1,2,\ldots,n-1\}} \sum_{j = i \mod n} t_k a_i b_j b_{\ell} + \sum_{i \neq \ell} \sum_{k \in \{1,2,\ldots,n-1\}} \sum_{j = i \mod n} t_k a_i \]

\[ = \sum_{i = \ell} \sum_{k \in \{1,2,\ldots,n-1\}} \sum_{j = i \mod n} t_k a_i b_j b_{\ell} + \sum_{i \neq \ell} \sum_{k \in \{1,2,\ldots,n-1\}} \sum_{j = i \mod n} t_k a_i \cdot 0 \]

\[ = \sum_{i = \ell} \sum_{k \in \{1,2,\ldots,n-1\}} \sum_{j = i \mod n} t_k a_i b_j b_{\ell} = \sum_{k = \lambda} t_k a_{\lambda} b_{\lambda} b_{\ell} \]

\[ (\text{by } (2)) \]

\[ = \sum_{k = \lambda} t_k b_{\ell} = t_{\lambda} b_{\ell} \]

(since \( \ell \in \{1,2,\ldots,n\} \))

Thus,

\[ t_{\lambda} b_{\ell} = \sum_{i \in \{1,2,\ldots,n\}} \sum_{k \in \{1,2,\ldots,n-1\}} \sum_{j = i \mod n} t_k a_i b_j b_{\ell} = 0. \]

Hence, (5) is proven.

Now,

\[ 1 = \sum_{k = 1}^{n} a_k b_k = \sum_{\ell = 1}^{n} a_{\ell} b_{\ell} \]

(9)

(here we renamed the summation index \( k \) as \( \ell \)).

Thus, for every \( \lambda \in \{1,2,\ldots,n-1\} \), we have

\[ t_{\lambda} = t_{\lambda} \cdot \frac{1}{\sum_{k = 1}^{n} a_k b_k} = t_{\lambda} \cdot \sum_{\ell = 1}^{n} a_{\ell} b_{\ell} = \sum_{\ell = 1}^{n} a_{\ell} t_{\lambda} b_{\ell} = \sum_{\ell = 1}^{n} a_{\ell} \cdot 0 = 0. \]

Thus, \( (t_1, t_2, \ldots, t_{n-1}) = 0. \) Therefore, Assertion 1 is proven.

Proof of Assertion 2. First, we are going to show that

\[ b_{\ell} v_\omega \in \langle s_1, s_2, \ldots, s_{n-1} \rangle_R \]

for any \( \ell \in \{1,2,\ldots,n\} \)

and any \( \omega \in \{1,2,\ldots,n\} \) satisfying \( \ell \neq \omega \). \hfill (10)
**Proof of (10).** Let \( \ell \in \{1, 2, \ldots, n\} \) and \( \omega \in \{1, 2, \ldots, n\} \) be such that \( \ell \neq \omega \).

Let \( \psi \) be the remainder of \( \omega - \ell - 1 \) upon division by \( n \). Then, \( \psi \in \{0, 1, \ldots, n-1\} \) and \( \psi \equiv \omega - \ell - 1 \mod n \).

Let \( k = \psi + 1 \). Then, \( k = \psi + 1 \in \{1, 2, \ldots, n\} \) (since \( \psi \in \{0, 1, \ldots, n-1\} \)) and \( \omega - \ell \equiv k \mod n \) (since \( k = \psi + 1 \equiv (\omega - \ell - 1) + 1 = \omega - \ell \mod n \)).

Now,

for every \( j \in \{1, 2, \ldots, n\} \), the assertions \( j - \ell \equiv k \mod n \) and \( j = \omega \) are equivalent. \( \square \)

The assertions \( \ell - \ell \equiv k \mod n \) and \( \ell = \omega \) are equivalent (by \( \square \)), applied to \( j = \ell \). Hence, the assertion \( \ell - \ell \equiv k \mod n \) is false (since the assertion \( \ell = \omega \) is false (since \( \ell \neq \omega \))). Thus, \( \ell - \ell \neq k \mod n \). Hence, \( k \neq \ell - \ell = \frac{j - \omega}{n} \in \mathbb{Z} \).

4**Proof of (6):** Let \( j \in \{1, 2, \ldots, n\} \).

Assume that \( j - \ell \equiv k \mod n \). Thus, \( j - \ell \equiv k \equiv \omega - \ell \mod n \), so that \( n \mid (j - \ell) - (\omega - \ell) = j - \omega \). Hence, \( \frac{j - \omega}{n} \in \mathbb{Z} \).

But \( j \in \{1, 2, \ldots, n\} \) and thus \( 0 < j \leq n \). Also, \( \omega \in \{1, 2, \ldots, n\} \) and thus \( 0 < \omega \leq n \).

Combining

\[
\frac{j - \omega}{n} > \frac{0 - n}{n} = -1
\]

and

\[
\frac{j - \omega}{n} < \frac{n - 0}{n} = 1
\]

we obtain \( \frac{j - \omega}{n} \in \mathbb{Z} \). This (combined with \( \frac{j - \omega}{n} \in \mathbb{Z} \)) yields \( \frac{j - \omega}{n} \in \mathbb{Z} \cap \mathbb{Z} = \{0\} \). Hence, \( \frac{j - \omega}{n} = 0 \), so that \( j - \omega = 0 \), and therefore \( j = \omega \).

Now, let us forget that we assumed that \( j - \ell \equiv k \mod n \). We thus have proven that \( j = \omega \) if \( j - \ell \equiv k \mod n \). In other words, we have proven the implication

\[
(j - \ell \equiv k \mod n) \implies (j = \omega).
\]

(12)

But the implication

\[
(j = \omega) \implies (j - \ell \equiv k \mod n)
\]

also holds (because if \( j = \omega \), then \( j - \ell = \omega - \ell \equiv k \mod n \)). Combining the implications \( \square \) and \( \square \), we obtain the logical equivalence

\[
(j - \ell \equiv k \mod n) \iff (j = \omega).
\]

In other words, the assertions \( j - \ell \equiv k \mod n \) and \( j = \omega \) are equivalent. This proves \( \square \).
0 \equiv n \mod n; \text{ thus, } k \neq n. \text{ This, combined with } k \in \{1, 2, \ldots, n\}, \text{ yields } k \in \{1, 2, \ldots, n\} \setminus \{n\} = \{1, 2, \ldots, n - 1\}. \text{ Thus, } s_k \text{ is well-defined.}

Now,

\[
b_\ell = \sum_{i,j \in \{1, 2, \ldots, n\}^2; j \equiv k \mod n} a_i b_i e_j
= b_\ell \sum_{i \in \{1, 2, \ldots, n\}; j \equiv k \mod n} a_i b_i e_j
= b_\ell \sum_{i \in \{1, 2, \ldots, n\}; j \equiv k \mod n} a_i b_i e_j
= \sum_{i \in \{1, 2, \ldots, n\}; j \equiv k \mod n} a_i b_i e_j \quad \text{(applied to } u = i \text{ and } v = \ell) \quad \text{(since } i \neq \ell) \quad \text{(by (2))}
= \sum_{i \in \{1, 2, \ldots, n\}; j \equiv k \mod n} a_i b_i e_j
= \sum_{i \in \{1, 2, \ldots, n\}; j \equiv k \mod n} a_i b_i e_j
= \sum_{i \in \{1, 2, \ldots, n\}; j \equiv k \mod n} a_i b_i e_j
= a_\ell b_\ell \sum_{j \in \{1, 2, \ldots, n\}; j \equiv k \mod n} e_j
= a_\ell b_\ell \sum_{j \in \{1, 2, \ldots, n\}; j \equiv k \mod n} e_j
= b_\ell \sum_{j \in \{1, 2, \ldots, n\}; j \equiv k \mod n} e_j
= b_\ell \sum_{j \in \{1, 2, \ldots, n\}; j = \omega} e_j
= b_\ell \sum_{j \in \{1, 2, \ldots, n\}; j = \omega} e_j
= b_\ell \sum_{j \in \{1, 2, \ldots, n\}; j = \omega} e_j
= b_\ell e_\omega,
\]

so that

\[
b_\ell e_\omega = b_\ell s_k \in \langle s_1, s_2, \ldots, s_{n-1} \rangle_R.
\]

Hence, (10) is proven.
Now, for every \( \omega \in \{1, 2, \ldots, n\} \), we have

\[
e^{\omega} = 1e^{\omega} = \sum_{\ell = 1}^{n} a_{\ell}b_{\ell}e^{\omega} \quad \text{(by (9))}
\]

\[
= \sum_{\ell \in \{1, 2, \ldots, n\}} a_{\ell}b_{\ell}e^{\omega} = \sum_{\ell \in \{1, 2, \ldots, n\}; \ell \neq \omega} a_{\ell}b_{\ell}e^{\omega} + \sum_{\ell = \omega} a_{\ell}b_{\ell}e^{\omega}
\]

\[
= \sum_{\ell \in \{1, 2, \ldots, n\}; \ell \neq \omega} a_{\ell}b_{\ell}e^{\omega} + a_{\omega} \begin{array}{c} \omega e^{\omega} \quad \text{(since)} \end{array} = b_{\omega}e^{\omega} = 0 \quad \text{(since)} \quad b_{\omega}e^{\omega} \in (b_1e_1, b_2e_2, \ldots, b_ne_n)_R
\]

\[
\subseteq \langle s_1, s_2, \ldots, s_{n-1} \rangle_R \quad \text{(since } \langle s_1, s_2, \ldots, s_{n-1} \rangle_R \text{ is an } R\text{-module).}
\]

(14)

From this, it easily follows that \( T/\langle b_1e_1, b_2e_2, \ldots, b_ne_n \rangle_R \subseteq \langle s_1, s_2, \ldots, s_{n-1} \rangle_R \) \( \nabla \)

This, combined with \( \langle s_1, s_2, \ldots, s_{n-1} \rangle_R \subseteq T/\langle b_1e_1, b_2e_2, \ldots, b_ne_n \rangle_R \) (which is obvious), yields \( \langle s_1, s_2, \ldots, s_{n-1} \rangle_R = T/\langle b_1e_1, b_2e_2, \ldots, b_ne_n \rangle_R \). Therefore, Assertion 2 is proven.

Now that both Assertions 1 and 2 are proven, we need only a trivial step to solve the problem:

The vectors \( s_1, s_2, \ldots, s_{n-1} \) are linearly independent (by Assertion 1) and generate the \( R\text{-module } T/\langle b_1e_1, b_2e_2, \ldots, b_ne_n \rangle_R \) (by Assertion 2). Hence,
$(s_1, s_2, \ldots, s_{n-1})$ is a basis of the $R$-module $T/\langle b_1 e_1, b_2 e_2, \ldots, b_n e_n \rangle_R$. Thus, the $R$-module $T/\langle b_1 e_1, b_2 e_2, \ldots, b_n e_n \rangle_R$ is a free $R$-module of rank $n - 1$ (because the basis $(s_1, s_2, \ldots, s_{n-1})$ consists of $n - 1$ vectors). Thus, the problem is solved.

**Remark.**

The problem solved above is a generalization of the “Advanced Problem A5715”, proposed in The American Mathematical Monthly, 1970, issue 2. More precisely, the problem in the Monthly is the particular case where $R$ is a polynomial ring and where $n = 3$; however, the problem also asks for a generalization, and I suspect that the generalization intended is precisely the generalized problem solved above.

I do not know if a solution has ever been published in the Monthly; nor do I understand the inside joke(?) that is the authorship of this problem.

My solution above looks like a magic trick; certainly, the definition of $s_k$ appears completely unmotivated. However, there is no true magic in it. It is merely a pedestrian (and explicit) way to rewrite an argument using orthogonal idempotents, which proceeds roughly as follows:

- First, we prove $[3]$. As a consequence, $a_u b_u$ is an idempotent for every $u \in \{1, 2, \ldots, n\}$.

- Thus, the elements $a_1 b_1$, $a_2 b_2$, $\ldots$, $a_n b_n$ are orthogonal idempotents. (We say that $n$ elements $q_1$, $q_2$, $\ldots$, $q_n$ of a commutative ring $R$ are orthogonal idempotents if they are idempotents and satisfy $[q_i q_j = 0$ for every two distinct elements $i$ and $j$ of $\{1, 2, \ldots, n\}]$.

) Moreover, $a_1 b_1$, $a_2 b_2$, $\ldots$, $a_n b_n$ form a complete system of orthogonal idempotents. (We say that $n$ orthogonal idempotents $q_1$, $q_2$, $\ldots$, $q_n$ in a commutative ring $R$ form a complete system of orthogonal idempotents if they satisfy $\sum_{i=1}^{n} q_i = 1$.)

We have $y = \sum_{j=1}^{n} r_j e_j = \sum_{\omega=1}^{n} r_\omega e_\omega$ (here we renamed the summation index $j$ as $\omega$) and thus

\[
\sum_{\omega=1}^{n} r_\omega e_\omega = \sum_{\omega=1}^{n} r_\omega \underbrace{e_\omega}_{(by \ [3])} \in \sum_{\omega=1}^{n} r_\omega \langle s_1, s_2, \ldots, s_{n-1} \rangle_R
\]

\[
\subseteq \langle s_1, s_2, \ldots, s_{n-1} \rangle_R \quad \text{(since $\langle s_1, s_2, \ldots, s_{n-1} \rangle_R$ is an $R$-module)}.
\]

Hence, $x = \overline{y} \in \langle s_1, s_2, \ldots, s_{n-1} \rangle_R$.

Now, let us forget that we fixed $x$. We thus have proven that $x \in \langle s_1, s_2, \ldots, s_{n-1} \rangle_R$ for every $x \in T/\langle b_1 e_1, b_2 e_2, \ldots, b_n e_n \rangle_R$. In other words, $T/\langle b_1 e_1, b_2 e_2, \ldots, b_n e_n \rangle_R \subseteq \langle s_1, s_2, \ldots, s_{n-1} \rangle_R$, qed.

\[6] It is not the only problem in the Monthly published by Anon from Erewhon-upon-Wabash. Problems E2155 and E2207 are other examples.

10
• Set \( c_i = a_i b_i \) for every \( i \in \{1, 2, \ldots, n\} \). Then, what we have just proven is that \( c_1, c_2, \ldots, c_n \) form a complete system of orthogonal idempotents.

• For every \( u \in \{1, 2, \ldots, n\} \), we have \( c_u = a_u b_u \) (by the definition of \( c_u \)) and \( c_u b_u = b_u \) (by \( (3) \)). Hence, for every \( u \in \{1, 2, \ldots, n\} \), we have \( \langle b_u e_u \rangle_R = \langle c_u e_u \rangle_R \). Thus, \( \langle b_1 e_1, b_2 e_2, \ldots, b_n e_n \rangle_R = \langle c_1 e_1, c_2 e_2, \ldots, c_n e_n \rangle_R \).

As a consequence of this, we can completely forget about \( a_1, a_2, \ldots, a_n \) and about \( b_1, b_2, \ldots, b_n \). All that we need to prove is that the \( R \)-module \( T/\langle c_1 e_1, c_2 e_2, \ldots, c_n e_n \rangle_R \) is a free \( R \)-module of rank \( n - 1 \), where \( c_1, c_2, \ldots, c_n \) are \( n \) elements of \( R \) that form a complete system of orthogonal idempotents.

• So let \( c_1, c_2, \ldots, c_n \) form a complete system of orthogonal idempotents in a commutative ring \( R \). Then, it is well-known that the ring \( R \) is isomorphic to the Cartesian product \( \prod_{i=1}^n (R/(1-c_i)R) \) of quotient rings, and that the isomorphism sends each \( c_i \) to the vector \((0, 0, \ldots, 0, 1, 0, 0, \ldots, 0)\) (with the 1 at the \( i \)-th position) in this Cartesian product. Moreover, every \( R \)-module \( M \) is isomorphic to the Cartesian product \( \prod_{i=1}^n (M/(1-c_i)M) \) as abelian groups, and each \( M/(1-c_i)M \) canonically becomes an \( R/(1-c_i)R \)-module. Better yet, we obtain an equivalence of categories between \( \text{Mod}_R \) and \( \prod_{i=1}^n \text{Mod}_{R/(1-c_i)R} \) (where \( \text{Mod}_S \) denotes the category of \( S \)-modules for a commutative ring \( S \), and where the product sign denotes the Cartesian product of categories). Any \( R \)-module \( M \in \text{Mod}_R \) corresponds to the \( n \)-tuple

\[
(M/(1-c_1)M, M/(1-c_2)M, \ldots, M/(1-c_n)M) \in \prod_{i=1}^n \text{Mod}_{R/(1-c_i)R}
\]

under this correspondence. If \( M \) is our \( R \)-module \( T/\langle c_1 e_1, c_2 e_2, \ldots, c_n e_n \rangle_R \), then the corresponding \( n \)-tuple

\[
(M/(1-c_1)M, M/(1-c_2)M, \ldots, M/(1-c_n)M)
\]

has the property that each \( M/(1-c_i)M \) is a free \( R/(1-c_i)R \)-module.

---

7More precisely, the isomorphism \( R \to \prod_{i=1}^n (R/(1-c_i)R) \) sends every \( r \in R \) to the \( n \)-tuple \((r_1, r_2, \ldots, r_n)\), where \( r_i \) is the projection of \( r \) onto the quotient ring \( R/(1-c_i)R \). The inverse map \( \prod_{i=1}^n (R/(1-c_i)R) \to R \) sends every \((r_1, r_2, \ldots, r_n) \in \prod_{i=1}^n (R/(1-c_i)R)\) to the element \( \sum_{i=1}^n c_i r_i' \), where \( r_i', r_1', r_2', \ldots, r_n' \) are (arbitrarily chosen) representatives of the residue classes \( r_1, r_2, \ldots, r_n \) in \( R \).
of rank $n-1$. From this, it is easy to conclude that $M = T/\langle c_1 e_1, c_2 e_2, \ldots, c_n e_n \rangle_R$ itself is a free $R$-module of rank $n-1$.

The reason why my solution above is not a direct elaboration of this argument, but rather an artificial reformulation, is the difficulty of formalizing this argument directly without much handwaving.

\[ \text{In fact, it is easy to see that } M/(1-c_i)M \text{ has basis } (\overline{e}_1, \overline{e}_2, \ldots, \overline{e}_{i-1}, \overline{e}_{i+1}, \ldots, \overline{e}_n), \text{ where } \overline{w} \text{ denotes the projection of a vector } w \in M \text{ onto } M/(1-c_i)M. \]