American Mathematical Monthly
Problem A5715 by Anon, Erewhon-upon-Wabash, generalized

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

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

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

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

Solution by Darij Grinberg.

First, notice that

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

[*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 [1], so that $b_u b_v = 0$ always holds, and thus, (2) is proven.]

Furthermore, we notice that

$$a_u b_u^2 = b_u \qquad \text{for any } u \in \{1, 2, \ldots, n\}. \tag{3}$$

[1] In fact,

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

[*Proof of (3).* Let $u \in \{1, 2, \ldots, n\}$. Then,

$$\underbrace{\sum_{v \in \{1,2,\ldots,n\}}}_{= \sum\limits_{v=1}^{n}} a_v b_v = \sum_{v=1}^{n} a_v b_v = \sum_{k=1}^{n} a_k b_k$$

(here we renamed the summation index v as k)

$$= 1$$

and thus

$$b_u \cdot \underbrace{\sum_{v \in \{1,2,\ldots,n\}} a_v b_v}_{=1} = b_u \cdot 1 = b_u.$$

Compared with

$$\begin{aligned} b_u \cdot \sum_{v \in \{1,2,\ldots,n\}} a_v b_v &= \sum_{v \in \{1,2,\ldots,n\}} a_v b_u b_v \\ &= \sum_{\substack{v \in \{1,2,\ldots,n\}; \\ v \neq u}} a_v \underbrace{b_u b_v}_{\substack{=0 \\ \text{(by (2)} \\ \text{(since } u \neq v \text{ (since } v \neq u)))}} + \underbrace{\sum_{\substack{v \in \{1,2,\ldots,n\}; \\ v = u}} a_v b_u b_v}_{\substack{= a_u b_u b_u \\ \text{(since } u \in \{1,2,\ldots,n\})}} \\ &= \underbrace{\sum_{\substack{v \in \{1,2,\ldots,n\}; \\ v \neq u}} a_v \cdot 0}_{=0} + a_u \underbrace{b_u b_u}_{= b_u^2} = a_u b_u^2, \end{aligned}$$

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 $T \diagup \langle b_1 e_1, b_2 e_2, \ldots, b_n e_n \rangle_R$. (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 $T \diagup \langle b_1 e_1, b_2 e_2, \ldots, b_n e_n \rangle_R$ by

$$s_k = \sum_{\substack{(i,j) \in \{1,2,\ldots,n\}^2; \\ j - i \equiv k \bmod n}} a_i b_i \overline{e_j}.$$

We are now going to prove two lemmata:

Assertion 1: Let $(t_1, t_2, \ldots, t_{n-1}) \in R^{n-1}$. If $\sum\limits_{k=1}^{n-1} t_k s_k = 0$, then $(t_1, t_2, \ldots, t_{n-1}) = 0$ (where 0 denotes the zero vector $\left(\underbrace{0, 0, \ldots, 0}_{n-1 \text{ zeroes}} \right) \in R^{n-1}$).

Assertion 2: We have $\langle s_1, s_2, \ldots, s_{n-1} \rangle_R = T \diagup \langle b_1 e_1, b_2 e_2, \ldots, b_n e_n \rangle_R$.

Proof of Assertion 1. Assume that $\sum\limits_{k=1}^{n-1} t_k s_k = 0$. Then,

$$0 = \underbrace{\sum_{k=1}^{n-1}}_{=\sum\limits_{k\in\{1,2,\ldots,n-1\}}} t_k \underbrace{s_k}_{=\sum\limits_{\substack{(i,j)\in\{1,2,\ldots,n\}^2;\\ j-i\equiv k \bmod n}} a_i b_i \overline{e_j}} = \sum_{k\in\{1,2,\ldots,n-1\}} t_k \sum_{\substack{(i,j)\in\{1,2,\ldots,n\}^2;\\ j-i\equiv k \bmod n}} a_i b_i \overline{e_j}$$

$$= \overline{\sum_{k\in\{1,2,\ldots,n-1\}} t_k \sum_{\substack{(i,j)\in\{1,2,\ldots,n\}^2;\\ j-i\equiv k \bmod n}} a_i b_i e_j}$$

$$= \overline{\underbrace{\sum_{(i,j)\in\{1,2,\ldots,n\}^2}}_{=\sum\limits_{j\in\{1,2,\ldots,n\}}\sum\limits_{i\in\{1,2,\ldots,n\}}} \sum_{\substack{k\in\{1,2,\ldots,n-1\};\\ j-i\equiv k \bmod n}} t_k a_i b_i e_j} = \overline{\underbrace{\sum_{j\in\{1,2,\ldots,n\}}}_{=\sum\limits_{j=1}^{n}} \sum_{i\in\{1,2,\ldots,n\}} \sum_{\substack{k\in\{1,2,\ldots,n-1\};\\ j-i\equiv k \bmod n}} t_k a_i b_i e_j}$$

$$= \overline{\sum_{j=1}^{n} \sum_{i\in\{1,2,\ldots,n\}} \sum_{\substack{k\in\{1,2,\ldots,n-1\};\\ j-i\equiv k \bmod n}} t_k a_i b_i e_j},$$

so that

$$\sum_{j=1}^{n} \sum_{i\in\{1,2,\ldots,n\}} \sum_{\substack{k\in\{1,2,\ldots,n-1\};\\ j-i\equiv k \bmod n}} t_k a_i b_i e_j \in \langle b_1 e_1, b_2 e_2, \ldots, b_n e_n \rangle_R$$

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

(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 $(r_1, r_2, \ldots, r_n) \in R^n$ such that

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

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

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

$$= \underbrace{\sum_{j=1}^{n} \sum_{i\in\{1,2,\ldots,n\}} \sum_{\substack{k\in\{1,2,\ldots,n-1\};\\ j-i\equiv k \bmod n}} t_k a_i b_i e_j}_{=\sum\limits_{j=1}^{n} r_j b_j e_j} - \sum_{j=1}^{n} r_j b_j e_j = \sum_{j=1}^{n} r_j b_j e_j - \sum_{j=1}^{n} r_j b_j e_j = 0.$$

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

$$\sum_{i\in\{1,2,\ldots,n\}} \sum_{\substack{k\in\{1,2,\ldots,n-1\}; \\ j-i\equiv k \bmod n}} t_k a_i b_i - r_j b_j = 0 \qquad \text{for every } j \in \{1, 2, \ldots, n\}.$$

[2] In other words,

$$\sum_{i\in\{1,2,\ldots,n\}} \sum_{\substack{k\in\{1,2,\ldots,n-1\}; \\ j-i\equiv k \bmod n}} t_k a_i b_i = r_j b_j \qquad \text{for every } j \in \{1, 2, \ldots, n\}. \tag{4}$$

Next, we are going to show that

$$t_\lambda b_\ell = 0 \text{ for any } \lambda \in \{1, 2, \ldots, n-1\} \text{ and any } \ell \in \{1, 2, \ldots, n\}. \tag{5}$$

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

Let $j = \phi + 1$. Then, $j = \phi + 1 \in \{1, 2, \ldots, n\}$ (since $\phi \in \{0, 1, \ldots, n-1\}$). Also, $j \equiv \lambda + \ell \bmod n$ (since $j = \underbrace{\phi}_{\equiv\lambda+\ell-1 \bmod n} + 1 \equiv (\lambda + \ell - 1) + 1 = \lambda + \ell \bmod n$), so that $j - \ell \equiv \lambda \bmod n$. Now,

$$\text{for every } k \in \{1, 2, \ldots, n-1\}, \text{ the assertions } j-\ell \equiv k \bmod n \text{ and } k = \lambda \text{ are equivalent.} \tag{6}$$

[3]

We have $\lambda \in \{1, 2, \ldots, n-1\}$, thus $n \nmid \lambda$, thus $\lambda \not\equiv 0 \bmod n$, hence $j \equiv \underbrace{\lambda}_{\not\equiv 0 \bmod n} + \ell \not\equiv 0 + \ell = \ell \bmod n$, thus $j \neq \ell$. Hence, (2) (applied to $u = j$ and

---

[2] *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 $\alpha_j = \sum_{i\in\{1,2,\ldots,n\}} \sum_{\substack{k\in\{1,2,\ldots,n-1\}; \\ j-i\equiv k \bmod n}} t_k a_i b_i - r_j b_j$, we obtain $\left(\sum_{i\in\{1,2,\ldots,n\}} \sum_{\substack{k\in\{1,2,\ldots,n-1\}; \\ j-i\equiv k \bmod n}} t_k a_i b_i - r_j b_j = 0 \text{ for every } j \in \{1, 2, \ldots, n\} \right)$ (since $\sum_{j=1}^{n} \left(\sum_{i\in\{1,2,\ldots,n\}} \sum_{\substack{k\in\{1,2,\ldots,n-1\}; \\ j-i\equiv k \bmod n}} t_k a_i b_i - r_j b_j \right) e_j = 0$), qed.

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

Assume that $j - \ell \equiv k \bmod n$. Then, $k \equiv j - \ell \equiv \lambda \bmod n$, so that $n \mid \lambda - k$. Thus, $\dfrac{\lambda - k}{n} \in \mathbb{Z}$.

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

$v = \ell$) shows that $b_j b_\ell = 0$. Now,

$$\underbrace{\sum_{i\in\{1,2,\ldots,n\}} \sum_{\substack{k\in\{1,2,\ldots,n-1\}; \\ j-i\equiv k \bmod n}} t_k a_i b_i}_{\substack{=r_j b_j \\ \text{(by (4))}}} b_\ell = r_j \underbrace{b_j b_\ell}_{=0} = r_j \cdot 0 = 0.$$

---

thus $0 < k < n$. Combining

$$\begin{aligned} \frac{\lambda - k}{n} &> \frac{0-n}{n} \qquad \text{(since } \lambda > 0 \text{ and } k < n\text{)} \\ &= -1 \end{aligned}$$

and

$$\begin{aligned} \frac{\lambda - k}{n} &< \frac{n-0}{n} \qquad \text{(since } \lambda < n \text{ and } k > 0\text{)} \\ &= 1, \end{aligned}$$

we obtain $\frac{\lambda - k}{n} \in \left]-1, 1\right[$. This (combined with $\frac{\lambda - k}{n} \in \mathbb{Z}$) yields $\frac{\lambda - k}{n} \in \mathbb{Z} \cap \left]-1, 1\right[= \{0\}$. Hence, $\frac{\lambda - k}{n} = 0$, so that $\lambda - k = 0$, and thus $k = \lambda$.

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

$$(j - \ell \equiv k \bmod n) \Longrightarrow (k = \lambda). \tag{7}$$

But the implication

$$(k = \lambda) \Longrightarrow (j - \ell \equiv k \bmod n) \tag{8}$$

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

$$(j - \ell \equiv k \bmod n) \Longleftrightarrow (k = \lambda).$$

In other words, the assertions $j - \ell \equiv k \bmod n$ and $k = \lambda$ are equivalent. This proves (6).

But on the other hand,

$$\sum_{i\in\{1,2,\ldots,n\}} \sum_{\substack{k\in\{1,2,\ldots,n-1\};\\ j-i\equiv k \bmod n}} t_k a_i b_i b_\ell$$

$$= \sum_{\substack{i\in\{1,2,\ldots,n\};\\ i=\ell}} \sum_{\substack{k\in\{1,2,\ldots,n-1\};\\ j-i\equiv k \bmod n}} t_k a_i b_i b_\ell + \sum_{\substack{i\in\{1,2,\ldots,n\};\\ i\neq\ell}} \sum_{\substack{k\in\{1,2,\ldots,n-1\};\\ j-i\equiv k \bmod n}} t_k a_i \underbrace{b_i b_\ell}_{\substack{=0\\ \text{(by (2)}\\ \text{(applied to } u=i \text{ and } v=\ell)\\ \text{(since } i\neq\ell))}}$$

$$= \sum_{\substack{i\in\{1,2,\ldots,n\};\\ i=\ell}} \sum_{\substack{k\in\{1,2,\ldots,n-1\};\\ j-i\equiv k \bmod n}} t_k a_i b_i b_\ell + \underbrace{\sum_{\substack{i\in\{1,2,\ldots,n\};\\ i\neq\ell}} \sum_{\substack{k\in\{1,2,\ldots,n-1\};\\ j-i\equiv k \bmod n}} t_k a_i \cdot 0}_{=0}$$

$$= \sum_{\substack{i\in\{1,2,\ldots,n\};\\ i=\ell}} \sum_{\substack{k\in\{1,2,\ldots,n-1\};\\ j-i\equiv k \bmod n}} t_k a_i b_i b_\ell = \underbrace{\sum_{\substack{k\in\{1,2,\ldots,n-1\};\\ j-\ell\equiv k \bmod n}}}_{\substack{=\sum\limits_{\substack{k\in\{1,2,\ldots,n-1\};\\ k=\lambda}}\\ \text{(by (6))}}} t_k \underbrace{a_\ell b_\ell b_\ell}_{\substack{=a_\ell b_\ell^2=b_\ell\\ \text{(by (3)}\\ \text{(applied to } u=\ell))}}$$

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

$$= \sum_{\substack{k\in\{1,2,\ldots,n-1\};\\ k=\lambda}} t_k b_\ell = t_\lambda b_\ell \qquad \left(\text{since } \lambda\in\{1,2,\ldots,n-1\}\right).$$

Thus,

$$t_\lambda b_\ell = \sum_{i\in\{1,2,\ldots,n\}} \sum_{\substack{k\in\{1,2,\ldots,n-1\};\\ j-i\equiv k \bmod n}} t_k a_i b_i b_\ell = 0.$$

Hence, (5) is proven.

Now,

$$1 = \sum_{k=1}^{n} a_k b_k = \sum_{\ell=1}^{n} a_\ell b_\ell \tag{9}$$

(here we renamed the summation index k as ℓ).

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

$$t_\lambda = t_\lambda \cdot \underbrace{1}_{=\sum\limits_{\ell=1}^{n} a_\ell b_\ell} = t_\lambda \cdot \sum_{\ell=1}^{n} a_\ell b_\ell = \sum_{\ell=1}^{n} a_\ell \underbrace{t_\lambda b_\ell}_{\substack{=0\\ \text{(by (5))}}} = \sum_{\ell=1}^{n} a_\ell \cdot 0 = 0.$$

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

$$b_\ell \overline{e_\omega} \in \langle s_1, s_2, \ldots, s_{n-1}\rangle_R \text{ for any } \ell\in\{1,2,\ldots,n\} \text{ and any } \omega\in\{1,2,\ldots,n\} \text{ satisfying } \ell\neq\omega. \tag{10}$$

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

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

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

Now,

for every $j \in \{1, 2, \ldots, n\}$, the assertions $j - \ell \equiv k \bmod n$ and $j = \omega$ are equivalent. (11)

[4]

The assertions $\ell - \ell \equiv k \bmod n$ and $\ell = \omega$ are equivalent (by (11), applied to $j = \ell$). Hence, the assertion $\ell - \ell \equiv k \bmod n$ is false (since the assertion $\ell = \omega$ is false (since $\ell \neq \omega$)). Thus, $\ell - \ell \not\equiv k \bmod n$. Hence, $k \not\equiv \ell - \ell =$

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

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

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

$$\begin{aligned} \frac{j - \omega}{n} &> \frac{0 - n}{n} \qquad \text{(since } j > 0 \text{ and } \omega \leq n\text{)} \\ &= -1 \end{aligned}$$

and

$$\begin{aligned} \frac{j - \omega}{n} &< \frac{n - 0}{n} \qquad \text{(since } j \leq n \text{ and } \omega > 0\text{)} \\ &= 1, \end{aligned}$$

we obtain $\dfrac{j - \omega}{n} \in \left]-1, 1\right[$. This (combined with $\dfrac{j - \omega}{n} \in \mathbb{Z}$) yields $\dfrac{j - \omega}{n} \in \mathbb{Z} \cap \left]-1, 1\right[= \{0\}$. Hence, $\dfrac{j - \omega}{n} = 0$, so that $j - \omega = 0$, and therefore $j = \omega$.

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

$$(j - \ell \equiv k \bmod n) \Longrightarrow (j = \omega). \tag{12}$$

But the implication

$$(j = \omega) \Longrightarrow (j - \ell \equiv k \bmod n) \tag{13}$$

also holds (because if $j = \omega$, then $\underbrace{j}_{=\omega} - \ell = \omega - \ell \equiv k \bmod n$). Combining the implications (12) and (13), we obtain the logical equivalence

$$(j - \ell \equiv k \bmod n) \Longleftrightarrow (j = \omega).$$

In other words, the assertions $j - \ell \equiv k \bmod n$ and $j = \omega$ are equivalent. This proves (11).

$0 \equiv n \bmod n$; thus, $k \neq n$. This, combined with $k \in \{1, 2, \ldots, n\}$, yields $k \in \{1, 2, \ldots, n\} \setminus \{n\} = \{1, 2, \ldots, n-1\}$. Thus, s_k is well-defined.

Now,

$$
\begin{aligned}
& b_\ell \\
& = \underbrace{\sum_{\substack{(i,j) \in \{1,2,\ldots,n\}^2; \\ j-i \equiv k \bmod n}}}_{s_k} a_i b_i \overline{e_j} \\
& = b_\ell \underbrace{\sum_{\substack{(i,j) \in \{1,2,\ldots,n\}^2; \\ j-i \equiv k \bmod n}}}_{= \sum\limits_{i \in \{1,2,\ldots,n\}} \sum\limits_{\substack{j \in \{1,2,\ldots,n\}; \\ j-i \equiv k \bmod n}}} a_i b_i \overline{e_j} = b_\ell \sum_{i \in \{1,2,\ldots,n\}} \sum_{\substack{j \in \{1,2,\ldots,n\}; \\ j-i \equiv k \bmod n}} a_i b_i \overline{e_j} \\
& = b_\ell \sum_{i \in \{1,2,\ldots,n\}} a_i b_i \sum_{\substack{j \in \{1,2,\ldots,n\}; \\ j-i \equiv k \bmod n}} \overline{e_j} \sum_{i \in \{1,2,\ldots,n\}} a_i b_i b_\ell \sum_{\substack{j \in \{1,2,\ldots,n\}; \\ j-i \equiv k \bmod n}} \overline{e_j} \\
& = \sum_{\substack{i \in \{1,2,\ldots,n\}; \\ i=\ell}} a_i b_i b_\ell \sum_{\substack{j \in \{1,2,\ldots,n\}; \\ j-i \equiv k \bmod n}} \overline{e_j} + \sum_{\substack{i \in \{1,2,\ldots,n\}; \\ i \neq \ell}} a_i \underbrace{b_i b_\ell}_{\substack{=0 \\ \text{(by (2)} \\ \text{(applied to } u=i \text{ and } v=\ell) \\ \text{(since } i \neq \ell))}} \sum_{\substack{j \in \{1,2,\ldots,n\}; \\ j-i \equiv k \bmod n}} \overline{e_j} \\
& = \sum_{\substack{i \in \{1,2,\ldots,n\}; \\ i=\ell}} a_i b_i b_\ell \sum_{\substack{j \in \{1,2,\ldots,n\}; \\ j-i \equiv k \bmod n}} \overline{e_j} + \underbrace{\sum_{\substack{i \in \{1,2,\ldots,n\}; \\ i \neq \ell}} a_i \cdot 0 \cdot \sum_{\substack{j \in \{1,2,\ldots,n\}; \\ j-i \equiv k \bmod n}} \overline{e_j}}_{=0} \\
& = \sum_{\substack{i \in \{1,2,\ldots,n\}; \\ i=\ell}} a_i b_i b_\ell \sum_{\substack{j \in \{1,2,\ldots,n\}; \\ j-i \equiv k \bmod n}} \overline{e_j} = \underbrace{a_\ell b_\ell b_\ell}_{\substack{=a_\ell b_\ell^2 = b_\ell \\ \text{(by (3)} \\ \text{(applied to } u=\ell))}} \sum_{\substack{j \in \{1,2,\ldots,n\}; \\ j-\ell \equiv k \bmod n}} \overline{e_j} \qquad (\text{since } \ell \in \{1, 2, \ldots, n\}) \\
& = b_\ell \underbrace{\sum_{\substack{j \in \{1,2,\ldots,n\}; \\ j-\ell \equiv k \bmod n}}}_{\substack{= \sum\limits_{\substack{j \in \{1,2,\ldots,n\}; \\ j=\omega}} \\ \text{(by (11))}}} \overline{e_j} = b_\ell \underbrace{\sum_{\substack{j \in \{1,2,\ldots,n\}; \\ j=\omega}} \overline{e_j}}_{\substack{=\overline{e_\omega} \\ \text{(since } \omega \in \{1,2,\ldots,n\})}} = b_\ell \overline{e_\omega},
\end{aligned}
$$

so that

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

Hence, (10) is proven.

Now, for every $\omega \in \{1, 2, \ldots, n\}$, we have

$$\begin{aligned}
\overline{e_\omega} = 1\overline{e_\omega} &= \underbrace{\sum_{\ell=1}^{n}}_{=\sum\limits_{\ell\in\{1,2,\ldots,n\}}} a_\ell b_\ell \overline{e_\omega} \qquad \text{(by (9))} \\
&= \sum_{\ell\in\{1,2,\ldots,n\}} a_\ell b_\ell \overline{e_\omega} = \sum_{\substack{\ell\in\{1,2,\ldots,n\};\\ \ell\neq\omega}} a_\ell b_\ell \overline{e_\omega} + \underbrace{\sum_{\substack{\ell\in\{1,2,\ldots,n\};\\ \ell=\omega}} a_\ell b_\ell \overline{e_\omega}}_{\substack{=a_\omega b_\omega \overline{e_\omega} \\ \text{(since } \omega\in\{1,2,\ldots,n\})}} \\
&= \sum_{\substack{\ell\in\{1,2,\ldots,n\};\\ \ell\neq\omega}} a_\ell b_\ell \overline{e_\omega} + a_\omega \underbrace{b_\omega \overline{e_\omega}}_{\substack{=\overline{b_\omega e_\omega}=0 \\ \text{(since} \\ b_\omega e_\omega \in \langle b_1e_1, b_2e_2, \ldots, b_ne_n\rangle_R)}} = \sum_{\substack{\ell\in\{1,2,\ldots,n\};\\ \ell\neq\omega}} a_\ell b_\ell \overline{e_\omega} + \underbrace{a_\omega \cdot 0}_{=0} \\
&= \sum_{\substack{\ell\in\{1,2,\ldots,n\};\\ \ell\neq\omega}} a_\ell \underbrace{b_\ell \overline{e_\omega}}_{\substack{\in\langle s_1, s_2, \ldots, s_{n-1}\rangle_R \\ \text{(by (10) (since } \ell\neq\omega))}} \in \sum_{\substack{\ell\in\{1,2,\ldots,n\};\\ \ell\neq\omega}} a_\ell \left\langle s_1, s_2, \ldots, s_{n-1}\right\rangle_R \\
&\subseteq \left\langle s_1, s_2, \ldots, s_{n-1}\right\rangle_R \qquad \left(\text{since } \left\langle s_1, s_2, \ldots, s_{n-1}\right\rangle_R \text{ is an } R\text{-module}\right).
\end{aligned} \tag{14}$$

From this, it easily follows that $T \diagup \langle b_1e_1, b_2e_2, \ldots, b_ne_n\rangle_R \subseteq \left\langle s_1, s_2, \ldots, s_{n-1}\right\rangle_R$ [5]. This, combined with $\left\langle s_1, s_2, \ldots, s_{n-1}\right\rangle_R \subseteq T \diagup \langle b_1e_1, b_2e_2, \ldots, b_ne_n\rangle_R$ (which is obvious), yields $\left\langle s_1, s_2, \ldots, s_{n-1}\right\rangle_R = T \diagup \langle b_1e_1, b_2e_2, \ldots, b_ne_n\rangle_R$. 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, …, s_{n-1} are linearly independent (by Assertion 1) and generate the R-module $T \diagup \langle b_1e_1, b_2e_2, \ldots, b_ne_n\rangle_R$ (by Assertion 2). Hence,

[5] *First proof of* $T \diagup \langle b_1e_1, b_2e_2, \ldots, b_ne_n\rangle_R \subseteq \left\langle s_1, s_2, \ldots, s_{n-1}\right\rangle_R$*:* We have proven that $\overline{e_\omega} \in \left\langle s_1, s_2, \ldots, s_{n-1}\right\rangle_R$ for every $\omega \in \{1, 2, \ldots, n\}$. Thus, $\left\langle \overline{e_1}, \overline{e_2}, \ldots, \overline{e_n}\right\rangle_R \subseteq \left\langle s_1, s_2, \ldots, s_{n-1}\right\rangle_R$. But $(e_1, e_2, \ldots, e_n)$ is a basis of the free R-module T. Thus, $T = \langle e_1, e_2, \ldots, e_n\rangle_R$, and therefore $T \diagup \langle b_1e_1, b_2e_2, \ldots, b_ne_n\rangle_R = \left\langle \overline{e_1}, \overline{e_2}, \ldots, \overline{e_n}\right\rangle_R$. Hence,

$$T \diagup \langle b_1e_1, b_2e_2, \ldots, b_ne_n\rangle_R = \left\langle \overline{e_1}, \overline{e_2}, \ldots, \overline{e_n}\right\rangle_R \subseteq \left\langle s_1, s_2, \ldots, s_{n-1}\right\rangle_R,$$

qed.

Second proof of $T \diagup \langle b_1e_1, b_2e_2, \ldots, b_ne_n\rangle_R \subseteq \left\langle s_1, s_2, \ldots, s_{n-1}\right\rangle_R$*:* Let $x \in T \diagup \langle b_1e_1, b_2e_2, \ldots, b_ne_n\rangle_R$. Then, there exists a $y \in T$ such that $x = \overline{y}$ (since $x \in T \diagup \langle b_1e_1, b_2e_2, \ldots, b_ne_n\rangle_R$). Consider this y.

But $(e_1, e_2, \ldots, e_n)$ is a basis of the free R-module T. Thus, $T = \langle e_1, e_2, \ldots, e_n\rangle_R$. Now, $y \in T = \langle e_1, e_2, \ldots, e_n\rangle_R = \left\{ \sum\limits_{j=1}^{n} r_je_j \mid (r_1, r_2, \ldots, r_n) \in R^n \right\}$ (by the definition of $\langle e_1, e_2, \ldots, e_n\rangle_R$). In other words, there exists some $(r_1, r_2, \ldots, r_n) \in R^n$ such that $y = \sum\limits_{j=1}^{n} r_je_j$. Consider this $(r_1, r_2, \ldots, r_n)$.

$(s_1, s_2, \ldots, s_{n-1})$ is a basis of the R-module $T \diagup \langle b_1 e_1, b_2 e_2, \ldots, b_n e_n \rangle_R$. Thus, the R-module $T \diagup \langle b_1 e_1, b_2 e_2, \ldots, b_n e_n \rangle_R$ 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[6].

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

  $$(q_i q_j = 0 \text{ for every two distinct elements } i \text{ and } j \text{ of } \{1, 2, \ldots, n\}).$$

) 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 $\sum\limits_{i=1}^{n} q_i = 1$.)

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

$$\overline{y} = \overline{\sum_{\omega=1}^{n} r_\omega e_\omega} = \sum_{\omega=1}^{n} r_\omega \underbrace{\overline{e_\omega}}_{\substack{\in \langle s_1, s_2, \ldots, s_{n-1} \rangle_R \\ \text{(by (14))}}} \in \sum_{\omega=1}^{n} r_\omega \langle s_1, s_2, \ldots, s_{n-1} \rangle_R$$

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

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 $x \in T \diagup \langle b_1 e_1, b_2 e_2, \ldots, b_n e_n \rangle_R$. In other words, $T \diagup \langle b_1 e_1, b_2 e_2, \ldots, b_n e_n \rangle_R \subseteq \langle s_1, s_2, \ldots, s_{n-1} \rangle_R$, 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.

- 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 $T \diagup \langle c_1 e_1, c_2 e_2, \ldots, c_n e_n \rangle_R$ 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 $\prod\limits_{i=1}^{n} \left(R \diagup (1 - c_i) R\right)$ 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.[7] Moreover, every R-module M is isomorphic to the Cartesian product $\prod\limits_{i=1}^{n} \left(M \diagup (1 - c_i) M\right)$ as abelian groups, and each $M \diagup (1 - c_i) M$ canonically becomes an $R \diagup (1 - c_i) R$-module. Better yet, we obtain an equivalence of categories between Mod_R and $\prod\limits_{i=1}^{n} \operatorname{Mod}_{R \diagup (1 - c_i) R}$ (where 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 $M \in \operatorname{Mod}_R$ corresponds to the n-tuple

$$\left(M \diagup (1 - c_1) M, M \diagup (1 - c_2) M, \ldots, M \diagup (1 - c_n) M\right) \in \prod_{i=1}^{n} \operatorname{Mod}_{R \diagup (1 - c_i) R}$$

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

$$\left(M \diagup (1 - c_1) M, M \diagup (1 - c_2) M, \ldots, M \diagup (1 - c_n) M\right)$$

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

[7] More precisely, the isomorphism $R \to \prod\limits_{i=1}^{n} \left(R \diagup (1 - c_i) R\right)$ 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 $R \diagup (1 - c_i) R$. The inverse map $\prod\limits_{i=1}^{n} \left(R \diagup (1 - c_i) R\right) \to R$ sends every $(r_1, r_2, \ldots, r_n) \in \prod\limits_{i=1}^{n} \left(R \diagup (1 - c_i) R\right)$ to the element $\sum\limits_{i=1}^{n} c_i r'_i$, where $r'_1,\ r'_2,\ \ldots,\ r'_n$ are (arbitrarily chosen) representatives of the residue classes $r_1,\ r_2,\ \ldots,\ r_n$ in R.

of rank $n-1$ [8]. From this, it is easy to conclude that $M = T \big/ \langle c_1 e_1, c_2 e_2, \ldots, c_n e_n \rangle_R$ 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.

[8] In fact, it is easy to see that $M \big/ (1-c_i)\, M$ has basis $(\overline{e_1}, \overline{e_2}, \ldots, \overline{e_{i-1}}, \overline{e_{i+1}}, \ldots, \overline{e_n})$, where $\overline{w}$ denotes the projection of a vector $w \in M$ onto $M \big/ (1-c_i)\, M$.