MAS511 2020 Spring Homework#07

Problem 1

Prove:

Theorem 1. *(PBW; Poincaré-Birkhoff-Witt) Let F be a field, L be an F-Lie algebra with a basis $\mathcal{B}$. Give a well-ordering on $\mathcal{B}$.*

A canonical monomial over $\mathcal{B}$ is a sequence $(x_1, \cdots, x_r)$ with $x_1 \leq \cdots \leq x_r$, $x_i \in \mathcal{B}$. For the natural map $i : L \to U(L)$, define $i(x_1, \cdots, x_r) := i(x_1) \cdots i(x_r)$. ($i()$ is an embedded image of $1_F \in F = T^0(L)$ to $U(L)$)

Then i is injective on the set of all canonical monomials, and the images form an F-basis of $U(L)$.

Proof

Notation: overline means embedded image from some $T^k(L)$ into the $U(L)$. i-th entry of $U(L)$ means the part of $T^i(L)$ of $U(L)$. Adjacent entry of i-th entry means the part of $T^{i+1}(L)$ or T^{i-1}. Higher entry than i-th means the part of $T^k(L)$ where $k > i$. Lower entry than i-th means the part of $T^k(L)$ where $k < i$. Index of the i-th entry of $U(L)$ is i. Tensor product term means an expression which has a form of $a_1 \otimes \cdots \otimes a_n$. The l-th item of a tensor product term $a_1 \otimes \cdots \otimes a_n$ is a_l.

Note, $U(L) = T(L)/I(L)$ where $I(L)$ is an ideal generated by $x \otimes y - y \otimes x - [x, y]$ for $x, y \in L$. In other words, in $U(L)$, $\overline{[x, y]} = \overline{x \otimes y - y \otimes x}$. $i : L \to U(L)$ is a map such that $x \mapsto x \in T^1_F(L) = L$.

(1) i is injective.

Before the proof, for $U(L)$,

- $\mathbf{x} = \overline{(0, \cdots, 0, x_1 \otimes \cdots \otimes x_r, 0, \cdots)}$ is 0 if $x_1 \otimes \cdots \otimes x_r$ is zero. Because non-zero elements of $I(L)$ contain at least two non-zero entries, $(0, \cdots, 0, x_1 \otimes \cdots \otimes x_r, 0, \cdots)$ cannot be in $I(L)$ if $x_1 \otimes \cdots \otimes x_r \neq 0$. Thus, the only possible case to make $\mathbf{x}$ zero is making $x_1 \otimes \cdots \otimes x_r$ zero. Since it's a tensor product over a field F, $\mathbf{x} = 0$ iff at least one of x_k is zero.
- Let $\mathbf{x} = \overline{(0, \cdots, 0, x_1 \otimes \cdots \otimes x_r, 0, \cdots)}$, and $\mathbf{y} = \overline{(0, \cdots, 0, y_1 \otimes \cdots \otimes y_r, 0, \cdots)}$. To make $\mathbf{x} - \mathbf{y}$ be zero, r-th entry of $\mathbf{x} - \mathbf{y}$, which is $x_1 \otimes \cdots \otimes x_r - y_1 \otimes \cdots \otimes y_r$ should be zero. To satisfy this condition, there are only two possible cases, which come from the equivalence relation of tensor product: (1) One of x_j and one of y_k are zero. In this case, each $\mathbf{x}$ and $\mathbf{y}$ become zero and the difference is also zero; (2) $x_k = y_k$ for every k. Because, To merge two tensor products $x_1 \otimes \cdots \otimes x_r$ and $y_1 \otimes \cdots \otimes y_r$, one entry x_k and y_k should be equal. Then, $x_1 \otimes \cdots \otimes x_r + y_1 \otimes \cdots \otimes y_r = (x_1 \otimes \cdots x_{k-1} - y_1 \otimes \cdots y_{k-1}) \otimes x_k \otimes (x_{k+1} \otimes \cdots x_r - y_{k+1} \otimes \cdots y_{ra})$. If $r-2$ more terms are same, we can repeat above process and obtain: $x_1 \otimes \cdots \otimes x_{l-1} \otimes (x_l - y_l) \otimes x_{l+1} \otimes \cdots \otimes x_r$. Then, if $x_l - y_l = 0$, this become zero. Otherwise, that cannot be zero. Therefore, $\mathbf{x} = \mathbf{y}$ iff $x_k = y_k$ for every k.

- Let $\mathbf{x} = \overline{(0, \cdots, 0, x_1 \otimes \cdots \otimes x_r, 0, \cdots)}$, and $\mathbf{y} = \overline{(0, \cdots, 0, y_1 \otimes \cdots \otimes y_s, 0, \cdots)}$ where $r \neq s$. Then, $\mathbf{x} - \mathbf{y}$ looks like $\overline{(0, \cdots, 0, y_1 \otimes \cdots \otimes y_s, 0, \cdots, 0, x_1 \otimes \cdots \otimes x_r, 0, \cdots)}$. If one of x_j and one of y_k are zero, it's a zero. If not, we need to note below for checking zero: (1) $\mathbf{x} - \mathbf{y}$ contains two non-zero entries; (2) The only possible case to reduce $\mathbf{x} - \mathbf{y}$ to zero is using the relation $x \otimes y - y \otimes x - [x, y]$. However, because $x \otimes y - y \otimes x$ and $[x, y]$ are in two different (but adjacent) entries. It means, there are two different conversion: subtraction of two tensor product terms into one term in the lower adjacent entry, and convert lower entry to the subtraction of two tensor product terms in the higher adjacent entry.

Let $r, s \in \mathbb{Z}^{\geq 0}$, $x_1, \cdots, x_r, y_1, \cdots, y_s \in \mathcal{B}$, and $x_1 \leq x_2 \leq \cdots \leq x_r$, $y_1 \leq y_2 \leq \cdots \leq y_s$. Let $\mathbf{x}$ be an embedded image of $(x_1, \cdots, x_r)$ into $U(L)$, and $\mathbf{y}$ be an embedded image of $(y_1, \cdots, y_s)$ into $U(L)$.

First, suppose that $r = s$. Then, $\mathbf{x} - \mathbf{y} = 0$ iff for every $x_k = y_k$ for each k. Thus $\mathbf{x} = \mathbf{y}$ iff $(x_1, \cdots, x_r) = (y_1, \cdots, y_s)$.

Next, suppose that $r \neq s$. WLOG, let's assume that $r > s$. Then,

$$\mathbf{x} - \mathbf{y} = \overline{(0, \cdots, 0, -y_1 \otimes \cdots \otimes y_s, 0, \cdots, 0, x_1 \otimes \cdots \otimes x_r, 0, \cdots)}$$

To convert r-th entry to $r-1$-th entry, there must be some $k \in \{1, \cdots, r-1\}$ such that $(x_1 \otimes \cdots \otimes x_r)$, $x_k \otimes x_{k+1} = a \otimes b - b \otimes a$ for some $a, b \in L$. (If so, we can reduce it as $[a, b]$). However, it's impossible. ($\because$ To reduce a subtraction of two tensor product terms into a tensor product term, If $a \otimes b - b \otimes a$ can be reduced to some $c \otimes d$, $a = fb$ or $b = fa$ for some $f \in F$. WLOG suppose that $a = fb$. Then, $a \otimes b - b \otimes a = f(b \otimes b) - f(b \otimes b) = 0$. However, $x_k \otimes x_{k+1} \neq 0$ since it's a tensor product of basis which are non-zero.) Thus, we cannot convert $\mathbf{x}$'s r-th entry to some lower entry. This show that $\mathbf{x} \neq \mathbf{y}$.

Therefore, i maps different elements of canonical basis into different elements of $U(L)$.

(2) The image of i generates $U(L)$

The element of $U(L)$ is a finite sum of embedded image of elements of $T^k(L)$ into $U(L)$. In other words, every non-zero element $\mathbf{x}$ of $U(L)$ can be represented as,

$$\mathbf{x} = \overline{f_0} + \sum_{j=1}^{n} \overline{\bigotimes_{k=1}^{m^j} f_{j,k} x_{j,k}}$$

for $n, m_j \in \mathbb{Z}^{\geq 0}$, $f_{j,k} \in F$ and $x_{j,k} \in L$. Then, for $f_j = \prod_{k=1}^{m^j} f_{j,k}$,

$$\mathbf{x} = \sum_{j=0}^{n} f_j \overline{\bigotimes_{k=1}^{m^j} x_{j,k}}$$

by the property of the tensor product. ($m_0 = 0$. $\overline{\bigotimes_{k=1}^{0} x_{j,k}} = \overline{1_F} = (1_F, 0, \cdots)$) Then, there may be some reverse ordered $x_{j,k}$ (where j satisfies $m_j \geq 2$), i.e. $x_{j,i} > x_{j,i+1}$. We know that,

$$\overline{x_{j,1} \otimes \cdots \otimes x_{j,i-1} \otimes (x_{j,i} \otimes x_{j,i+1} - x_{j,i+1} \otimes x_{j,i} - [x_{j,i}, x_{j,i+1}]) \otimes x_{j,i+2} \otimes \cdots \otimes x_{j,m_j}} \in I$$

Thus,

$$\begin{aligned} &\overline{x_{j,1} \otimes \cdots \otimes x_{j,i-1} \otimes x_{j,i} \otimes x_{j,i+1} \otimes x_{j,i+2} \otimes \cdots \otimes x_{j,m_j}} \\ =& -\overline{x_{j,1} \otimes \cdots \otimes x_{j,i-1} \otimes x_{j,i+1} \otimes x_{j,i} \otimes x_{j,i+2} \otimes \cdots \otimes x_{j,m_j}} \\ &-\overline{x_{j,1} \otimes \cdots \otimes x_{j,i-1} \otimes [x_{j,i}, x_{j,i+1}] \otimes x_{j,i+2} \otimes \cdots \otimes x_{j,m_j}} \end{aligned}$$

Using this relation, we can change an order of some two adjacent tensor product terms in the j-th summand. Therefore, by repeating reordering from the highest entry, we can assume that $x_{j,i} \leq x_{j,i+1}$ for every j, i. (This proecss halts because $\mathbf{x}$ is a finite sum.)

Then,

$$\begin{aligned} \mathbf{x} &= \sum_{j=0}^{n} \overline{f_j \bigotimes_{k=1}^{m^j} x_{j,k}} \\ &= \sum_{j=0}^{n} f_j \overline{\bigotimes_{k=1}^{m^j} x_{j,k}} \\ &= \sum_{j=0}^{n} f_j i\left(x_{j,1}, \cdots, x_{j,m_j}\right) \end{aligned}$$

Therefore, the image of i generates $U(L)$.

(3) The image of i is linearly independent

Let $\mathbf{x} \in U(L)$. Suppose that

$$\begin{aligned} \mathbf{x} &= \sum_{j=1}^{m} a_j i(x_{j,1}, \cdots, x_{j,m_j}) \\ &= \sum_{j=1}^{n} b_j i(y_{j,1}, \cdots, y_{j,n_j}) \end{aligned}$$

for $m, m_j, n, n_j \in \mathbb{Z}^{\geq 0}$, $a_j, b_j \in F \setminus \{0_F\}$, $x_{j,k}, y_{j,k} \in L$, $x_{j,k} \leq x_{j,k+1}$, $y_{j,k} \leq y_{j,k+1}$.

By reordering and inserting some summand with zero coefficients, we can make $x_{j,k} = y_{j,k}$ and $a_j, b_j \in F$. Thus, let's assume that

$$\begin{aligned} \mathbf{x} &= \sum_{j=1}^{n} a_j i(x_{j,1}, \cdots, x_{j,n_j}) \\ &= \sum_{j=1}^{n} b_j i(x_{j,1}, \cdots, x_{j,n_j}) \end{aligned}$$

where $i(x_{j,1}, \cdots, x_{j,n_j})$ are distinct. Then,

$$0 = \sum_{j=1}^{n} (a_j - b_j) i(x_{j,1}, \cdots, x_{j,n_j})$$

Suppose that $a_j \neq b_j$ for some j. Let $c_j = a_j - b_j$. Then, some c_j may be zero. By removing zero coefficient summands and reordering,

$$0 = \sum_{j=1}^{n'} c_j i(x_{j,1}, \cdots, x_{j,n'_j}) \quad \cdots (*)$$

where c_j are non-zero. Let p be the highest index of non-zero entry of $(*)$. If p-th entry of $(*)$ is just a single non-zero coefficient tensor product term, as we showed above, it cannot be reduced to the lower entry. It means, $(*)$ is non-zero. Suppose that p-th entry of $(*)$ is a sum of multiple non-zero coefficient tensor product term. However, if they don't have at least $p-1$ common items for tensor product, the sum cannot be reduced to a single tensor product term. In this case, the sum cannot be zero. Suppose that each summands of p-th entry of $(*)$ have common items of tensor products except l-th item. Since $(x_{j,1}, \cdots, x_{j,n'_j})$ are distinct, l-th items of each summands of p-th entry of $(*)$ are distinct. Then, the p-th entry of $(*)$ is reduced into

$$x_1 \otimes \cdots \otimes x_{k-1} \otimes y \otimes x_{k+1} \otimes \cdots \otimes x_p$$

where each x_j are common items of each tensor product term in the p-th entry of $(*)$, and y is a linear combination of l-th items of each sumamnds of p-th entry of $(*)$. Since y is a linear combination of distinct elements of $\mathcal{B}$ with non-zero coefficient, y is non-zero. Also, each tensor product summand of the p-th entry of $(*)$ cannot be reduced into the $p-1$-th entry of $(*)$. ($\because$ If two distinct $(x_1, \cdots, x_i, x_{i+1}, \cdots, x_p)$ and $(x_1, \cdots, x_{i+1}, x_i, \cdots, x_p)$ are included in the linear combination of p-th entry, we may use $a \otimes b - b \otimes a = [a, b]$ to reduce the p-th entry into $p-1$-th entry. However, in this case, since x_k must be ordered by $\leq$, in this case, $x_i \leq x_{i+1}$ and $x_{i+1} \leq x_i$. Then, $x_i = x_{i+1}$. However, each entry is a linear combination of different tensor products, $(x_1, \cdots, x_i, x_{i+1}, \cdots, x_p) \neq (x_1, \cdots, x_{i+1}, x_i, \cdots, x_p)$. It's a contradiction.) Therefore, $(*)$ cannot be zero, and it's a contradiction because we assumed that $(*) = 0$.

Therefore, every element of $U(L)$ can be represented by the unique linear combination of images of i. □

Problem 2

Theorem 2. *Let R be PID, M be finitely generated R-modules. Then $M \simeq R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$. for some $a_i \in R$ such that $a_1 \mid a_2 \mid \cdots \mid a_m$. The number r is unique and $a_1, \cdots, a_m$ are uniquely decided up to units in R.*

Let $x_1, \cdots, x_n \in M$ be a set of generators of M as an R-Mod.

Then, we can choose a generating set such that n to be minimum.

Define a surjective R-mod homomorphism $\phi : R^n \to M$ given by $(b_1, \cdots, b_n) \mapsto \sum_i b_i x_i$. Here $\ker\phi \subset R^n$ is a submodule of free module R^n over the PID R, by the previous theorem, it is free of rank $\leq n$, say m.

Also by the previous theorem, we can choose a basis $y_1, \cdots, y_n \in R^n$ and $a_1 \mid \cdots \mid a_m \in R$ such that $a_1y_1, \cdots, a_my_m \in \ker\phi$ and this set gives a basis for $\ker\phi$. Then

$$\begin{aligned} M \simeq R^n/\ker\phi &= (Ry_1 \oplus \cdots \oplus Ry_n)/(Ra_1y_1 \oplus \cdots \oplus Ra_my_m \oplus 0 \cdots) \\ &\simeq R/(a_1) \oplus \cdots \oplus R/(a_m) \oplus R^{n-m} \end{aligned}$$

Show that the uniqueness part.

Proof

Let $\mathrm{Tor}(M)$ be a torsion R-submodule of M. In other words, $\mathrm{Tor}(M) = \{m \in M \mid \exists r \in R \setminus \{0\} : rm = 0\}$.

Also, let's denote $a \sim b$ is $a = ub$ for some unit $u \in R$.

Suppose that there are $r, s \in \mathbb{Z}^{\geq 0}$ and $a_1 \mid a_2 \mid \cdots \mid a_m \in R$, $b_1 \mid \cdots \mid b_n \in R$ such that

$$\begin{aligned} M &\simeq R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m) \\ &\simeq R^s \oplus R/(b_1) \oplus \cdots \oplus R/(b_n) \end{aligned}$$

For convinience, let's denote

$$A_1 = R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$$

$$A_2 = R^s \oplus R/(b_1) \oplus \cdots \oplus R/(b_n)$$

Since $M \simeq A_1 \simeq A_2$, $\mathrm{Tor}(M) \simeq \mathrm{Tor}(A_1) \simeq \mathrm{Tor}(A_2)$. And, $M/\mathrm{Tor}(M) \simeq A_1/\mathrm{Tor}(A_1) \simeq A_2/\mathrm{Tor}(A_2)$.

Since R is a PID (thus ID), there is no zero divisors in R. In other words, for every nonzero $r \in R$, $rs \neq 0$ for every $s \in R \setminus \{0\}$. Then, for $\mathbf{x} \in A_1$ such that

$$\mathbf{x} = (x_1, \cdots, x_r, \overline{y_1}, \cdots, \overline{y_m})$$

by multiplicating by a_m

$$\begin{aligned} a_m\mathbf{x} &= (a_mx_1, \cdots, a_mx_r, a_m\overline{y_1}, \cdots, a_m\overline{y_m}) \\ &= (a_mx_1, \cdots, a_mx_r, 0, \cdots, 0) \end{aligned}$$

since $a_k \mid a_m$ for each $k = 1, \cdots, m$. Also, each rx_k is non-zero for $r \in R \setminus \{0\}$ if x_k is non-zero. Thus,

$$\mathrm{Tor}(A_1) = 0^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m) \simeq R/(a_1) \oplus \cdots \oplus R/(a_m)$$

$$A_1/\mathrm{Tor}(A_1) = R^r \oplus 0 \oplus \cdots \oplus 0 \simeq R^r$$

In the same way,

$$\mathrm{Tor}(A_2) \simeq R/(b_1) \oplus \cdots \oplus R/(b_n)$$

$$A_2/\mathrm{Tor}(A_2) \simeq R^s$$

First, $R^r \simeq A_1/\mathrm{Tor}(A_1) \simeq A_2/\mathrm{Tor}(A_2) \simeq R^s$. Then, the free rank of R^r, r, should be equal to the free rank of R^s, s. Thus, $r = s$.

Next,

$$\begin{aligned} A_1' = R/(a_1) \oplus \cdots \oplus R/(a_m) &\simeq \mathrm{Tor}(A_1) \\ &\simeq \mathrm{Tor}(A_2) \simeq R/(b_1) \oplus \cdots \oplus R/(b_n) = A_2' \end{aligned}$$

Let $(x_1, \cdots, x_m) \in A_1'$. Then, $a_m x_k = 0$ for each $k = 1, \cdots, m$, because $x_k \in R/(a_k)$ and $a_k \mid a_m$. Thus, every element of A_1' becomes zero by multiplicating by a_m. Since $A_1' \simeq A_2'$, every element of A_2' becomes zero by multiplicating by a_m too. It means, for every $r \in R$, $a_m r + (b_n) = a_m(r + (b_n)) = (b_n)$ and $a_m r \in (b_n)$. This shows $(b_n) \subseteq (a_m)$.

We can do this process from the A_2': since every element of A_2' becomes zero by multiplication by b_n, every element of A_1' becomes zero by multiplication by b_n, and this implies $(a_m) \subseteq (b_n)$.

Then, we know that $(a_m) = (b_n)$. This implies $a_m \sim b_n$.

Let $j \in \{1, \cdots, m\}$ be the minimal integer such that $a_j \sim a_{j+1} \sim \cdots \sim a_m$. And let $k \in \{1, \cdots, n\}$ be the minimal integer such that $b_k \sim b_{k+1} \sim \cdots \sim b_n$. Then, we known

$$(a_j) = (a_{j+1}) = \cdots = (a_m) = (b_n) = (b_{n-1}) = \cdots = (b_k)$$

Suppose that $j = 1$. Then, every elements of A_1' and A_2' should be zero by multiplication by a_m. It means k should be 1 too. Then,

$$A_1' \simeq \oplus_{i=1}^m R/(a_m) \simeq \oplus_{i=1}^n R/(a_m) \simeq A_2' \qquad \cdots (*)$$

. In this case, $m = n$ must hold.

If $j > 1$, since there is an element of A_1' which are not zero after the multiplication by a_m, there is an element of A_2' which are not zero after the multiplication by a_m too. Thus, $k > 1$.

Let's define $D(r; M) = \{0\} \cup \{m \in M \mid sm = 0 \text{ iff } r \mid s \in R\}$ for $r \in R$ and $M \in \mathrm{Ob}(R-\mathrm{Mod})$. Then, $D(r; M) \subseteq M$.

In this case,

$$D(a_m; A_1') \simeq R/(a_j) \oplus \cdots \oplus R/(a_m)$$

$$A_1'/D(a_m; A_1') \simeq R/(a_1) \oplus \cdots \oplus R/(a_{j-1})$$

$$D(a_m; A_2') \simeq R/(b_k) \oplus \cdots \oplus R/(b_n)$$

$$A_2'/D(a_m; A_2') \simeq R/(b_1) \oplus \cdots \oplus R/(b_{k-1})$$

Note that $D(a_m; A_1') \simeq D(a_m; A_2')$ since $A_1' \simeq A_2'$. Thus,

$$\oplus_{i=j}^m R/(a_m) \simeq \oplus_{i=k}^n R/(a_m) \qquad \cdots (*)$$

and $m - j + 1 = n - k + 1$. Also, $A_1'/D(a_m; A_1') \simeq A_2'/D(a_m; A_2')$. Thus, let's take $A_i'' = A_i'/D(a_m; A_i')$ for each $i = 1, 2$, repeat the above process for A_1'' and A_2''. Since the numbers of direct summands are strictly decreasing, this process halt at some time.

After the repetition, we know that,

- There are $0 = j_0 < j_1 < \cdots < j_p = m$ such that $a_{j_{i-1}} \not\sim a_{j_{i-1}+1} \sim a_{j_{i-1}+2} \sim \cdots \sim a_{j_i-1} \sim a_{j_i} \not\sim a_{j_i+1}$ for each i.
- There are $0 = k_0 < k_1 < \cdots < k_q = m$ such that $b_{k_{i-1}} \not\sim b_{k_{i-1}+1} \sim b_{k_{i-1}+2} \sim \cdots \sim b_{k_i-1} \sim b_{k_i} \not\sim b_{k_i+1}$ for each i.
- $p = q$. It's because p and q are the number of repition of above process.
- $j_i - j_{i-1} = k_i - k_{i-1}$ for every i. It's because of $(*)$.
- $m = n$. Because of above properties.
- $a_i \sim b_i$ for every i. It can be shown by above 5 properties and counting from the last element using the fact that for each process, the last element of $\{a_k\}$ and $\{b_k\}$ associate.

Therefore, it shows that $m = n$ and $a_i \sim b_i$ for each $i = 1, \cdots, m$.

In conclusion, if

$$\begin{aligned} M &\simeq R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m) \\ &\simeq R^s \oplus R/(b_1) \oplus \cdots \oplus R/(b_n) \end{aligned}$$

$r = s$, $m = n$ and $a_i = b_i$ for each $i = 1, \cdots, m$. □

Problem 3

Give an example of an integral domain R of dimension ≥ 2, where the first theorem fails: namely M is a free of finite rank, and $N \subset M$ is a submodule, but N is not free.

Proof

$R = \mathbb{Z}[x]$. It's not a PID, because the ideal $(2, x)$ is not a principal ideal. (Instead, it's a UFD because a polynomial ring of UFD is UFD.)

Let $M = R$ be a R-module. Since $M = R \simeq R^1$, M is free of rank 1.

Take $N = (2, x)$. Since it's an finitely generated ideal of M, N is a submodule of M.

Let's show that N is not free.

Suppose that N is free. Note that free modules should have a basis. Let $\mathcal{B}$ be a basis of N. Since $N \neq 0$, $\mathcal{B} \neq \emptyset$ trivially.

Suppose that $\mathcal{B} = \{b\}$. If $\deg b \geq 1$, there is no $r \in \mathbb{Z}[x]$ such that $rb = 2$ since $rb = 0$ or $\deg rb = \deg r + \deg b \geq \deg b = 1 > 0 = \deg 2$. If $\deg b = 0$, $b = 2n$ for some $n \in \mathbb{Z}$. However, in this case, there is no $r \in \mathbb{Z}[x]$ such that $rb = x$, because every coefficient of rb is multiplications by 2. Therefore, $|\mathcal{B}| \geq 2$.

As above, if $\mathcal{B}$ contains only elements of degree greater than 0, or if $\mathcal{B}$ contains only elements of degree 0, $\mathcal{B}$ cannot generate N. Thus, there are $b_1, b_2 \in \mathcal{B}$ such that $\deg b_1 = 0$, $\deg b_2 > 0$. However, in this case, $b_1 \cdot b_2 - b_2 \cdot b_1 = 0$. This shows that $\mathcal{B}$ is not linearly independent.

Therefore, there is no basis $\mathcal{B}$ of $(2, x)$ as an $\mathbb{Z}[x]$-module. It means, the ideal $(2, x)$ cannot be free. □

Problem 4

Let L be a Lie algebra over a field F.

(1) For an F-vector space M, find the natural definition of an L-module over the Lie algebra L. (Hint: you need something similar to that of the Jacobi identity.)

(2) Prove that an L-module M is naturally an $U(L)$-module for the associative F-algebra $U(L)$ in the ordinary sense.

(3) Prove that there is a natural equivalence of categories $L - \mathrm{Mod} \leftrightarrow U(L) - \mathrm{Mod}$

Proof of (1)

Note: M is an abelian group, F acts of M. L is a F-vector space.

For a ring R, we know that R-module M with an action $\cdot : R \times M \to M$ should satisfies, for $r, s \in R$, $m, n \in M$,

$$r \cdot (s \cdot m) = (rs) \cdot m$$

$$(r + s) \cdot m = r \cdot m + s \cdot m$$

$$r \cdot (m + n) = r \cdot m + r \cdot n$$

The below two are linearly, and the first one is associativity.

Let L be a Lie algebra over a field F and M be an F-vector space. Then, if M can be called as a L-module, it may need to satisfy linearlity and associativity.

However, L is not associative. More specifically, there is a Jacobi identity: for $\mathbf{j}, \mathbf{k}, \mathbf{l} \in L$,

$$[\mathbf{j}, [\mathbf{k}, \mathbf{l}]] + [\mathbf{k}, [\mathbf{l}, \mathbf{j}]] + [\mathbf{l}, [\mathbf{j}, \mathbf{k}]] = 0$$

Suppose that $\mathbf{m} \in M$ and $\cdot : L \times M \to M$ is an action. We want to replace $\mathbf{l}$ to $\mathbf{m}$. To achieve this, make above terms into the form of $[-, \mathbf{l}]$.

$$\begin{aligned} 0 = [\mathbf{j}, [\mathbf{k}, \mathbf{l}]] + [\mathbf{k}, [\mathbf{l}, \mathbf{j}]] + [\mathbf{l}, [\mathbf{j}, \mathbf{k}]] &= [\mathbf{j}, [\mathbf{k}, \mathbf{l}]] + [\mathbf{k}, -[\mathbf{j}, \mathbf{l}]] - [[\mathbf{j}, \mathbf{k}], \mathbf{l}] \\ &= [\mathbf{j}, [\mathbf{k}, \mathbf{l}]] - [\mathbf{k}, [\mathbf{j}, \mathbf{l}]] - [[\mathbf{j}, \mathbf{k}], \mathbf{l}] \end{aligned}$$

Then, change $\mathbf{l}$ to $\mathbf{m} \in M$ and $[-, \mathbf{n}]$ into $- \cdot \mathbf{n}$ for any $\mathbf{n} \in M$:

$$\begin{aligned} 0 &= [\mathbf{j}, [\mathbf{k}, \mathbf{l}]] - [\mathbf{k}, [\mathbf{j}, \mathbf{l}]] - [[\mathbf{j}, \mathbf{k}], \mathbf{l}] \\ &= [\mathbf{j}, \mathbf{k} \cdot \mathbf{m}] - [\mathbf{k}, \mathbf{j} \cdot \mathbf{m}] - [\mathbf{j}, \mathbf{k}] \cdot \mathbf{m} \\ &= \mathbf{j} \cdot (\mathbf{k} \cdot \mathbf{m}) - \mathbf{k} \cdot (\mathbf{j} \cdot \mathbf{m}) - [\mathbf{j}, \mathbf{k}] \cdot \mathbf{m} \end{aligned}$$

By add $[\mathbf{j}, \mathbf{k}] \cdot \mathbf{m}$ to the both side, we obtain

$$[\mathbf{j}, \mathbf{k}] \cdot \mathbf{m} = \mathbf{j} \cdot (\mathbf{k} \cdot \mathbf{m}) - \mathbf{k} \cdot (\mathbf{j} \cdot \mathbf{m})$$

This is a property looks like associativity for L-module.

Linearity is almost same as the R-module.

Thus, we can say that a F-vector space M is a L-module for an action $\cdot : L \times M \to M$ if it satisfies

$$[\mathbf{k}, \mathbf{l}] \cdot \mathbf{m} = \mathbf{k} \cdot (\mathbf{l} \cdot \mathbf{m}) - \mathbf{l} \cdot (\mathbf{k} \cdot \mathbf{m})$$

$$(\mathbf{k} + \mathbf{l}) \cdot \mathbf{m} = \mathbf{k} \cdot \mathbf{m} + \mathbf{l} \cdot \mathbf{m}$$

$$\mathbf{l}\cdot(\mathbf{m}+\mathbf{n})=\mathbf{l}\cdot\mathbf{m}+\mathbf{l}\cdot\mathbf{n}$$

$$f(\mathbf{l}\cdot\mathbf{m})=(f\mathbf{l})\cdot\mathbf{m}=\mathbf{l}\cdot(f\mathbf{m})$$

for every $f\in F$, every $\mathbf{k},\mathbf{l}\in L$ and every $\mathbf{m},\mathbf{n}\in M$.

Proof of (2)

Suppose that some structure A over a field F acts on some module M with $\cdot : A\times M\to M$. In this case, we want to extend the action to $* : (A\otimes_F A)\times M\to M$. Maybe, the most natural way to defined $*$ is,

$$(a\otimes b)*m=a\cdot(b\cdot m)$$

for each generator $(a\otimes b)$ of $A\otimes_F A$. Since $\otimes$ and $\cdot$ satisfies linearity, $*$ also have linearity. But tensor product itself does not have any product between them, thus we cannot say anything about associativity of $*$.

However, in the tensor algebra $T_F(A)$, we have a concatenation product. Let $a_1\otimes\cdots\otimes a_n\in T_F^n(A)$ and $\overline{a_1\otimes\cdots\otimes a_n}$ be an embedded image of $a_1\otimes\cdots\otimes a_n$ in $T_F(A)$. In this case, let

$$\overline{a_1\otimes\cdots\otimes a_n}*m=a_1\cdot(\cdots(a_n\cdot m))$$

Then, for $a_1\otimes\cdots\otimes a_n\in T_F^n(A)$ and $b_1\otimes\cdots\otimes b_l\in T_F^l(A)$,

$$\begin{aligned}\overline{a_1\otimes\cdots\otimes a_n}*(\overline{b_1\otimes\cdots\otimes b_l}*m)&=a_1*(a_2*(\cdots(a_n*(b_1*(\cdots(b_l*m))))))\\&=\overline{a_1\otimes\cdots\otimes a_n\otimes b_1\otimes\cdots\otimes b_l}*m\\&=\left(\overline{a_1\otimes\cdots\otimes a_n}\cdot\overline{b_1\otimes\cdots\otimes b_l}\right)*m\end{aligned}$$

Thus, this action is associative as an action of associative structure.

Let L be a Lie algebra, and M be a L-module (See (1)). Note that each element of $U(L)$ can be represented as:

$$\sum_{j=1}^{n}\overline{\bigotimes_{k=1}^{l_j}a_{j,k}}$$

for $n,l_j\in\mathbb{Z}^{\geq 0}$, $a_{j,k}\in L$. (If $l_j=0$, $\bigotimes_{k=1}^{l_j}a_{j,k}$ is some element of $F=T^0(L)$. Overline means embedded image into the $U(L)$.) Then, let's define an action of $U(L)$ on M as,

$$\left(\sum_{j=1}^{n}\overline{\bigotimes_{k=1}^{l_j}a_{j,k}}\right)\cdot m=\sum_{j=1}^{n}(a_{j,1}\cdot(\cdots(a_{j,l_j}\cdot m)))$$

First, we should check this is well-defined. Note that there are some equivalence relation of $U(L)$:

- $a\otimes b+a\otimes c=a\otimes(b+c)$. For $m\in M$,

$$\begin{aligned}\overline{a\otimes b+a\otimes c}\cdot m&=\overline{a\otimes b}\cdot m+\overline{a\otimes c}\cdot m\\&=a\cdot(b\cdot m)+a\cdot(c\cdot m)\\&=a\cdot(b\cdot m+c\cdot m)\\&=a\cdot(b\cdot m+c\cdot m)\\&=a\cdot((b+c)\cdot m)=\overline{a\otimes(b+c)}\cdot m\end{aligned}$$

- $a \otimes c + b \otimes c = (a+b) \otimes c$. In the similar way above, we can show that

  $$\overline{a \otimes c + b \otimes c} \cdot m = \overline{(a+b) \otimes c} \cdot m$$

  for $m \in M$.

- $f(a \otimes b) = (fa) \otimes b = a \otimes (fb)$ for $f \in F$. Then, by linearity of action of L on M, for any $m \in M$,

  $$\begin{aligned} \overline{(fa) \otimes b} \cdot m &= fa \cdot (b \cdot m) \\ &= f(a \cdot (b \cdot m)) = f(\overline{a \otimes b} \cdot m) \\ &= a \cdot (fb \cdot m) \\ &= \overline{a \otimes fb} \cdot m \end{aligned}$$

- $\overline{a \otimes b - b \otimes a - [a,b]} = 0$. In this case, Jacobi-identity-like associativity of L-action helps us: for $m \in M$,

  $$\begin{aligned} \overline{a \otimes b - b \otimes a - [a,b]} \cdot m &= \overline{a \otimes b} \cdot m - \overline{b \otimes a} \cdot m - \overline{[a,b]} \cdot m \\ &= a \cdot (b \cdot m) - b \cdot (a \cdot m) - [a,b] \cdot m \\ &= [a,b] \cdot m - [a,b] \cdot m = 0 \end{aligned}$$

Therefore, by properties of tensor product and pseudo associativity(?) of L-action, the $U(L)$-action is well-defined.

Then, it satisfies all properties of associative algebra action:

- $\mathbf{a} \cdot (\mathbf{b} \cdot \mathbf{m}) = (\mathbf{ab}) \cdot \mathbf{m}$ for $\mathbf{a}, \mathbf{b} \in U(L)$, $\mathbf{m} \in M$. It holds because as we shown at the top of the proof, for the concatenation product of $U(L)$, this kind of associativity hold.

- $(\mathbf{a} + \mathbf{b}) \cdot \mathbf{m} = \mathbf{a} \cdot \mathbf{m} + \mathbf{b} \cdot \mathbf{m}$ for $\mathbf{a}, \mathbf{b} \in U(L)$, $\mathbf{m} \in M$. This is directly from the definition of the action. (Since the $U(L)$-action takes a sum of embedded images of tensor products into a sum of value of module which obtained from L-action.)

- $\mathbf{a}\cdot(\mathbf{m}+\mathbf{n}) = \mathbf{a}\cdot\mathbf{m} + \mathbf{a}\cdot\mathbf{n}$ for $\mathbf{a}\in U(L)$, $\mathbf{m},\mathbf{n}\in M$. Let $\mathbf{a} = \sum_{j=1}^{n}\overline{\bigotimes_{k=1}^{l_j} a_{j,k}}$. Then,

$$\begin{aligned}
\mathbf{a}\cdot(\mathbf{m}+\mathbf{n}) &= \left(\sum_{j=1}^{n}\overline{\bigotimes_{k=1}^{l_j} a_{j,k}}\right)\cdot(\mathbf{m}+\mathbf{n}) \\
&= \sum_{j=1}^{n}\overline{\bigotimes_{k=1}^{l_j} a_{j,k}}\cdot(\mathbf{m}+\mathbf{n}) \\
&= \sum_{j=1}^{n} a_{j,1}(\cdots(a_{j,l_j}\cdot(\mathbf{m}+\mathbf{n}))) \\
&= \sum_{j=1}^{n} a_{j,1}(\cdots(a_{j,l_j-1}\cdot(a_{j,l_j}\cdot\mathbf{m}+a_{j,l_j}\cdot\mathbf{n}))) \\
&= \cdots \\
&= \sum_{j=1}^{n}\big(a_{j,1}(\cdots(a_{j,l_j}\cdot\mathbf{m})) + a_{j,1}(\cdots(a_{j,l_j}\cdot\mathbf{n}))\big) \\
&= \sum_{j=1}^{n}\overline{\bigotimes_{k=1}^{l_j} a_{j,k}}\cdot\mathbf{m} + \sum_{j=1}^{n}\overline{\bigotimes_{k=1}^{l_j} a_{j,k}}\cdot\mathbf{n} \\
&= \mathbf{a}\cdot\mathbf{m}+\mathbf{a}\cdot\mathbf{n}
\end{aligned}$$

- $f(\mathbf{a}\cdot\mathbf{m}) = f\mathbf{a}\cdot\mathbf{m} = \mathbf{a}\cdot f\mathbf{m}$ for $f\in F$, $\mathbf{a}\in U(L)$, $\mathbf{m}\in M$. It can be shown as: first, express $f\mathbf{a}\cdot\mathbf{m}$ as a sum of form of $f(a_1\otimes\cdots\otimes a_p)\cdot\mathbf{m}$, then it's, $f(a_1\cdot(\cdots(a_p\cdot\mathbf{m})))$ by the definition, use the property of L-action such that $f\mathbf{l}\cdot\mathbf{m} = \mathbf{l}\cdot f\mathbf{m}$ p-times, then we obtain $(a_1\cdot(\cdots(a_p\cdot f\mathbf{m})))$ and it can be resoted into $\mathbf{a}\cdot f\mathbf{m}$

Thus, we can extend L-module M to the $U(L)$-module.

Note that this is a unique extension of L-module to the $U(L)$-module. Because, if $F : L-\text{Mod}\to U(L)-\text{Mod}$ is a extension, F should preserve all objects and F preserve the behavior of action for the elements of $T_F^1(L) = L$ on M. Then, because of associativity, for $a,b\in L$, $\overline{a}\overline{b} = \overline{a\otimes b}\in T_F^2(L)$ holds, and $\overline{a}\cdot(\overline{b}\cdot m) = (\overline{a}\overline{b})\cdot m = \overline{a\otimes b}\cdot m$ should holds. Repeating this process, we obtain the above definition of action.

The proof of naturality is in the next part.

Proof of (3)

Let $F : L-\text{Mod}\to U(L)-\text{Mod}$ be a functor such that F maps each L-module into the $U(L)$-module preserving every object and morhpisms, but just changing the action as in the proof of (2).

In other words, for every $M,N\in L-\text{Mod}$ and every homomorhpism $\varphi : M\to N$, $F(M) = M$ in the sense of a set and $F(\varphi)=\varphi$ in the sense of a set map.

First, F is well-defeined as a map of objects, because we showed that for every L-module M, M is a $U(L)$-module.

Also, F is essentially surjective. Let M be an $U(L)$-module. Then, we can define a L-module action as,

$$\mathbf{l}\cdot\mathbf{m} = \bar{\mathbf{l}}\cdot\mathbf{m}$$

where $\mathbf{l}\in L$, $\mathbf{m}\in M$ and overline means the embeded image into the $U(L)$. Then, we can easily show that this action satisfies all properties which L-module must satisfy: linearity is trivial, $[\mathbf{k},\mathbf{l}]\cdot\mathbf{m} =$

$\mathbf{k}\cdot(\mathbf{l}\cdot\mathbf{m}) - \mathbf{l}\cdot(\mathbf{k}\cdot\mathbf{m})$ is hold because $\overline{[\mathbf{k},\mathbf{l}]} = \overline{\mathbf{k}\otimes\mathbf{l} - \mathbf{l}\otimes\mathbf{k}}$ and $\overline{\mathbf{k}\otimes\mathbf{l}}\cdot\mathbf{m} = \mathbf{k}\cdot(\mathbf{l}\cdot\mathbf{m})$. Thus, M is in $L-\text{Mod}$. And in this case, $F(M)$ is the given M, because we showed that L-module is extended to the $U(L)$-module in the unique way. This shows that F is essentially surjective.

F as a map of morphisms is well-defined. It's because $U(L)$-action is just a sum of results of L-actions. More specifically, let $\varphi : M \to N$ be an L-module homomorphism. Then, for $m, n \in M$ $\varphi(m+n) = \varphi(m) + \varphi(n)$ holds. For $m \in M$ and $\sum_{j=1}^{n} \overline{\bigotimes_{k=1}^{l_j} a_{j,k}} \in U(L)$

$$\begin{aligned}
\varphi\left(\left(\sum_{j=1}^{n}\overline{\bigotimes_{k=1}^{l_j} a_{j,k}}\right)\cdot m\right) &= \varphi\left(\sum_{j=1}^{n} a_{j,1}\cdot(\cdots(a_{j,l_j}\cdot m))\right)\\
&= \sum_{j=1}^{n} a_{j,1}\cdot(\cdots(a_{j,l_j}\cdot\varphi(m)))\\
&= \left(\sum_{j=1}^{n}\overline{\bigotimes_{k=1}^{l_j} a_{j,k}}\right)\cdot\varphi(m)
\end{aligned}$$

Thus, every L-module homomorphism is a $U(L)$-module homomorphism. Suppsoe that $\varphi : M \to N$ is an $U(L)$-module homomorphism. Then, for $m, n \in M$ $\varphi(m+n) = \varphi(m) + \varphi(n)$ holds trivially. For $m \in M$ and $l \in L$,

$$\varphi(l\cdot m) = \varphi(\bar{l}\cdot m) = \bar{l}\cdot\varphi(m) = l\cdot\varphi(m)$$

Thus every $U(L)$-module homomorphism is a L-module homomorphism.

Also, the above shows that there is 1-1 correspondence between L-module homomorphism and $U(L)$-module homomorphism. Therefore, F is fully faithful.

Then, this F is a functor because,

- $F(\text{Id}_M) = \text{Id}_{F(M)}$. Note F preserved every object and morphism. Thus, image of identity function by F is an identity function. ($F(\text{Id}_M) = \text{Id}_M = \text{Id}_{F(M)}$)

- $F(f\circ g) = F(f)\circ F(g)$. Composition of homomorphisms is same to the composition of set functions. Since F preserved morhpisms, $F(f\circ g) = f\circ g = F(f)\circ F(g)$ holds.

Therefore, we find a fully faithful and essentially surjective functor from $L-\text{Mod}$ to $U(L)-\text{Mod}$. Therefore, F is an equivalenec between $L-\text{Mod}$ and $U(L)-\text{Mod}$. □

Problem 5

Let R be commutative ring with 1. Regard the group of units $R^\times$ as a $\mathbb{Z}$-module. Consider the tensor algebra $T_{\mathbb{Z}}(R^\times)$, and let $I \subset T_{\mathbb{Z}}(R^\times)$ be the two-sided ideal generated by elements of the form $a \otimes (1-a)$ (where $a, 1-a \in R^\times$).

Consider the graded ring $K_*^M(R) := T_{\mathbb{Z}}(R^\times)/I$ and the image of the degree n part of $T(R^\times)$ is written $K_n^M(R)$. The former $K_*^M(R)$ is called the Milnor K-ring of R, and the latter $K_n^M(R)$ is called the n-th Milnor K-group of R.

Let $n \geq 2$ and let R be a finite field. Prove that $K_n^M(R) = 0$. (Hint: Recall $R^\times$ is cyclic.)

proof

Let $n = |R^\times|$ and $\mathbb{n} = \{0, \cdots, n-1\}$.

Since R is a finite field, every element except 0 are unit. For $a \in R \setminus \{0\}$, $1 - a = 0$ iff $a = 1$. Thus, $1 - a$ is a unit if $a \in R \setminus \{0, 1\}$.

Since $R^\times$ is finite, cyclic, let $R^\times = \langle g \rangle$. Then, every element of $R^\times$ can be represented as g^k for $k \in \mathbb{Z}$. Let's denote $k \cdot g = g^k$. Note that 1 in $R^\times$ is $0 \cdot g = g^0$.

Then, for arbitrary $a, b \in R^\times$, $a = \alpha \cdot g$, $b = \beta \cdot g$ and $a \otimes b = (\alpha \cdot g) \otimes (\beta \cdot g) = \alpha\beta(g \otimes g)$. It means, for every element $\tau \in R^\times \otimes_{\mathbb{Z}} R^\times$,

$$\begin{aligned}\tau &= \sum_{k=1}^{m} (\alpha_k \cdot g) \otimes (\beta_k \cdot g) \\ &= \left(\sum_{k=1}^{m} \alpha_k \beta_k\right)(g \otimes g)\end{aligned}$$

Thus, every element of $R^\times \otimes_{\mathbb{Z}} R^\times$ can be represented as $m \cdot (g \otimes g)$ for some $m \in \mathbb{Z}$.

Therefore, to show $K_2^M(R)$ is zero, it's enough to show that $g \otimes g$ is zero in $K_2^M(R)$.

Let's show $g \otimes g \in I$.

Before the proof of above claim, we note some important facts. First, let $-^* : R \to R$ such that $x^* = 1 - x$. This is a dual operator (i.e. $(x^*)^* = x$), since $1 - (1 - x) = x$ for every $x \in R$. It means, every element of R must be paired with exactly one element of R (it can be itself) by the operator. Also, let's denote $R' = R^\times \setminus \{0\}$. Then, $-^*$ is closed in R', because $0^* = 1$.

The first case is $R \simeq F_{2^m}$ for some $m \in \mathbb{N}$. It's the only case such that n is odd.

If $m = 1$, $R^\times = \{1\}$. Then, $g = 1$, which is an identity of $R^\times$. Thus, $g \otimes g \in I$ since it's a zero in the tensor algebra.

Suppose that $m = 2$. Then, $R^\times = \langle g \rangle = \{g^0, g^1, g^2\}$. Then, $(g^1)^*$ should be g^1 or g^2. Thus, $g^1 \otimes (g^1)^* = g \otimes g$ or $2(g \otimes g)$, and one of them is contained in I. If $g \otimes g \in I$, we are done. Since $2(2(g \otimes g)) = 4(g \otimes g) = g \otimes g$, $g \otimes g \in I$ if $2(g \otimes g) \in I$.

Suppose that $m > 2$. Let $S = \{k \in \mathbb{n} \mid k \cdot g = g^a(g^a)^* \text{ for some } g^a \in R'\}$. Let's show that the GCD of S is 1 or 2. Suppose that for the prime number $p \geq 3$, p divides every elements of S. In other words, for every $g^a \in R'$ and $g^b = (g^a)^*$, ab should be divides by p. That means, for every $g^a \in R'$ and $g^b = (g^a)^*$, $p \mid a$ or $p \mid b$. Therefore, at least $\lceil \frac{n-1}{2} \rceil$ elements of $\mathbb{n} \setminus \{0\}$ should be multiplications of p. However, in $\mathbb{n}$, there are at most $\lfloor \frac{n-1}{p} \rfloor$ elements which are multiplications of p. Thus, it's a contradiction. Also, if $p = 4$, we can make the same argument and we obtain the fact that 4 cannot divide all elements of S. Therefore, only 1 or 2 may divides all elements of S and GCD of S is 1 or 2. Note that for every $g^a \in R'$ and $g^b = (g^a)^*$, $g^a \otimes (g^a)^* = ab(g \otimes g)$. In other words, $S = \{k \in \mathbb{n} \mid k(g \otimes g) = g^a \otimes (g^a)^* \text{ for some } g^a \in R'\}$. And, GCD of S is 1 or 2 implies that by taking linear combination of $g^a(g^a)^* \in R'$, we obtain $g \otimes g$ or $2(g \otimes g)$. In other words, $g \otimes g \in I$ or $2(g \otimes g) \in I$. If $g \otimes g \in I$, we are done. If $2(g \otimes g) \in I$, since n is odd, for $k = \lceil n/2 \rceil = \frac{n+1}{2}$,

$$2k(g \otimes g) = ((n+1) \cdot g) \otimes g = g \otimes g + (n \cdot g) \otimes g = g \otimes g \in I$$

as $R^\times$ is a group of order n.

Next, let's consider the case of $R \simeq F_{p^m}$ for some prime $p \geq 3$ and $m \in \mathbb{N}$. Let

$$\begin{aligned} S &= \{k \in \mathbb{n} \mid k \cdot g = g^a(g^a)^* \text{ for some } g^a \in R'\} \\ &= \{k \in \mathbb{n} \mid k(g \otimes g) = g^a \otimes (g^a)^* \text{ for some } g^a \in R'\} \end{aligned}$$

as the previous case. Note that n is even and $|R'|$ is odd. Let's show that the GCD of S is 1. Suppose that there is a prime number p such that p divides every element of S. Then, for every $g^a \in R'$ and $g^b = (g^a)^*$, $p \mid a$ or $p \mid b$. Thus, at least $\lceil \frac{|R'|}{2} \rceil = \lceil \frac{n-1}{2} \rceil = \frac{n}{2}$ elements of $\mathbb{n} \setminus \{0\}$ must be divides by p. First, if $p = 2$, it's impossible, because, $\mathbb{n} \setminus \{0\} = \{1, 2, \cdots, n-1\}$ contains only $\frac{n}{2} - 1$ even elements, but we need at least $\lceil \frac{n-1}{2} \rceil = n$ elements. Also, if $p \geq 3$, $\mathbb{n} \setminus \{0\}$ contains at most $\lfloor \frac{n-1}{p} \rfloor$ elements of multiplication of p. Thus, we cannot have n elements of multiplication of p. Therefore, any prime numbers cannot divide every elements of S. This shows that GCD of S is 1. In other words, we obtain $g \otimes g$ from some linear combination of $g^a \otimes (g^a)^*$ of R'. Thus, $g \otimes g \in I$.

Then, since every element of $K_2^M(R)$ is generated by $g \otimes g$, $K_2^M(R) \subseteq I$. It implies $K_2^M(R) = 0$.

Let $l \in \mathbb{Z}^{\geq 3}$ and suppose that $K_k^M(R) = 0$ for every $2 \leq k < l$. By the definition of T, all elements of $K_l^M(R)$ is generated by the tensor product $a \otimes b$ where $a \in K_i^M(R)$ and $b \in K_{l-i}^M(R)$ for some $i \in \{1, \cdots, l-1\}$. WLOG, suppose that $i \geq l - i$. Then, $i \geq \frac{l}{2} \geq \frac{3}{2}$. Since i is an integer, $i \geq 2$. Then, by induction hypothesis, $a = 0$ because $a \in K_i^M(R) = 0$. Because tensor product with 0 is zero, $a \otimes b = 0$. Therefore, $K_l^M(R)$ is generated by 0 and it implies $K_l^M(R) = 0$.

In conclusion, for every $l \in \mathbb{Z}^{\geq 2}$, $K_l^M(R) = 0$. □