Noncommutative Algebra - 6th homework

Benjamin Benčina, 27192018

16. marec 2021

Ex. 1:

(a) Find all inner automorphisms of the first Weyl algebra $\mathcal{A}_1 = k\langle x, y \mid [y, x] = 1\rangle$.

Recall that an inner automorphism is an automorphism with the property that there exists an element $\alpha \in \mathcal{A}_1$ such that

$$\Phi_\alpha(z) = \alpha z \alpha^{-1}$$

for all $z \in \mathcal{A}_1$. From the above it is clear that $\alpha \in \mathcal{A}_1^{-1}$, so let us first determine what $\mathcal{A}_1^{-1}$ even is. The answer is rather easy, since the elements of $\mathcal{A}_1$ are essentially polynomials. Indeed, every element of $\mathcal{A}_1$ is of the form

$$z = \sum_{i,j=0}^{n,m} a_{ij} x^i y^j$$

since the defining relation $[y, x] = 1$ gives us a way to swap x and y by $yx = xy + 1$. Hence $\mathcal{A}_1^{-1} = k^{-1}$. The question is now whether we have that Φ_α, defined by $x \mapsto \alpha x \alpha^{-1}$ and $y \mapsto \alpha y \alpha^{-1}$, is an (inner) automorphism for all $\alpha \in k^{-1}$, to which the answer is trivially affirmative, since elements from k are by definition in $Z(\mathcal{A}_1)$. Moreover, for the same reason we have that $\Phi_\alpha = \Phi_1 = id$ (for all α which are not annihilated by a possible non-zero characteristic of k). So we have found the only inner automorphism – the identity id.

(b) Find an outer automorphism of $\mathcal{A}_1$.

Consider a linear automorphism Φ defined by $x \mapsto -y$ and $y \mapsto x$, which is well-defined since

$$\begin{vmatrix} 0 & 1 \\ -1 & 0 \end{vmatrix} = 1 \neq 0$$

Let us check the defining relation of $\mathcal{A}_1$ indeed holds

$$\Phi(y)\Phi(x) - \Phi(x)\Phi(y) = x(-y) - (-y)x = yx - xy = 1$$

This automorphism clearly cannot be inner.

Ex. 2: For the following group algebras we will decide whether they are semisimple. If the answer is affirmative, we will find its decomposition into simple algebras. Otherwise, we will find a basis of their Jacobson radical.

(a) $\mathbb{Z}_3[C_4]$: Clearly, we have $\operatorname{char} \mathbb{Z}_3 = 3$ and $|C_4| = 4$, so by Maschke's Theorem this group algebra is semisimple. Moreover, $\mathbb{Z}_3[C_4] \cong \mathbb{Z}_3[a]/(a^4 - 1)$ (the quotient of the polynomial ring), so any element can be written as

$$\alpha_0 1 + \alpha_1 a + \alpha_2 a^2 + \alpha_3 a^3$$

By Wedderburn's Theorem we have that this group algebra is isomorphic to a product of matrices over division rings, but $\mathbb{Z}_3[C_4]$ is clearly commutative of dimension 4, so it is either isomorphic

to $\mathbb{Z}_3^4$ or is itself a division ring (there are no matrices in the decomposition). Let us test when elements from this group algebra have a multiplicative inverse. We are solving

$$(\alpha_0 1 + \alpha_1 a + \alpha_2 a^2 + \alpha_3 a^3)(\beta_0 1 + \beta_1 a + \beta_2 a^2 + \beta_3 a^3) = 1$$

From this we obtain a system of equations that is represented by

$$Ab = \begin{bmatrix} \alpha_0 & \alpha_3 & \alpha_2 & \alpha_1 \\ \alpha_1 & \alpha_0 & \alpha_3 & \alpha_2 \\ \alpha_2 & \alpha_1 & \alpha_0 & \alpha_3 \\ \alpha_3 & \alpha_2 & \alpha_1 & \alpha_0 \end{bmatrix} \begin{bmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

We notice that for e.g. $1 + a^2$ we get a matrix of rank 2, which should be obvious since

$$(1 + a^2)(a^2 - 1) = (a^4 - 1) = 0$$

Hence this cannot be a division ring and we get

$$\mathbb{Z}_3[C_4] \cong \mathbb{Z}_3^4$$

(b) $\underline{\mathbb{Z}_3[C_6]}$: This time $\operatorname{char}\mathbb{Z}_3$ divides $|C_6|$, so by the converse to Maschke's Theorem[1] this group algebra is not semisimple. Again, we have that $\mathbb{Z}_3[C_6] \cong \mathbb{Z}_3[a]/(a^6 - 1)$ but this time $a^6 - 1 = (a^2 - 1)^3$, so $a^2 - 1$ is not merely a zero divisor but also a nilpotent. Hence the ideal $(a^2 - 1)$ is nil and thus contained in the Jacobson radical. When we factor it out we get $\mathbb{Z}_3[a]/(a^2 - 1)$, which is by Maschke's Theorem semisimple and therefore J-semisimple. Since neither $a - 1$ nor $a + 1$ are nilpotent, we have $\operatorname{rad}\mathbb{Z}_3[C_6] = (a^2 - 1)$.

(c) $\underline{\mathbb{Z}_3[S_3]}$: By the argument from (b), this group algebra is not semisimple. We have

$$\mathbb{Z}_3[S_3] = \left\{ \alpha_0 id + \alpha_1 (12) + \alpha_2 (123) + \alpha_3 (123)^2 \alpha_4 (12)(123) + \alpha_5 (123)(12) \;\middle|\; \alpha_i \in \mathbb{Z}_3 \right\}$$

We quickly notice that

$$((123) - id)^3 = (123)^3 - 3(123)^2 + 3(123) - id^3 = id - id = 0$$

in $\mathbb{Z}_3$ coefficients. Therefore as above the ideal $((123) - id)$ is nil and hence contained in the Jacobson radical. Once we factor it out we get $\{\alpha_0 id + \alpha_1 (12)\}$, which is isomorphic to $\mathbb{Z}_3[a]/(a^2 - 1)$ and by Maschke's Theorem semisimple (and hence J-semisimple). We get $\operatorname{rad}\mathbb{Z}_3[S_3] = ((123) - id)$.

(d) $\underline{\mathbb{Q}[S_3]}$: By Maschke's Theorem this algebra is semisimple, since $\operatorname{char}\mathbb{Q} = 0$. To obtain the simple parts we follow the example proof from the lectures. By Wedderburn's Theorem, we have that $\mathbb{Q}[S_3] \cong \prod_{i=1}^{n} M_{n_i}(D_i)$, where D_i are division rings that contain $\mathbb{Q}$. Of course $\dim_{\mathbb{Q}} \mathbb{Q}[S_3] = |S_3| = 6$, so for every i we have $\dim_{\mathbb{Q}} D_i < \infty$, so this excludes all p-adic or real extensions. Since if there exists i such that $\dim_{\mathbb{Q}} D_i \geq 2$ and $n_i \geq 2$ then $\dim_{\mathbb{Q}} M_{n_i}(D_i) = n_i^2 \dim_{\mathbb{Q}} D_i \geq 8 > 6$, we have that all D_i can only be $\mathbb{Q}$, so either $\mathbb{Q}[S_3] \cong \mathbb{Q}^6$ or $\mathbb{Q}[S_3] \cong M_2(\mathbb{Q}) \times \mathbb{Q}^2$. The former is commutative, which is a contradiction as S_3 is not Abelian, so the latter case must necessarily hold.

(e) $\underline{\mathbb{C}[S_4]}$: Again this algebra is semisimple, since $\operatorname{char}\mathbb{C} = 0$. The proof from (d) is simplified by the fact that $\mathbb{C}$ is algebraically closed, so $\mathbb{C}[S_4] \cong \prod_{i=1}^{n} M_{n_i}(\mathbb{C})$. Since $\dim_{\mathbb{C}} \mathbb{C}[S_4] = |S_4| = 24$, we have quite a few possibilities on how to assign n_i's. The highest perfect square below 24 is $4^2 = 16$, so the possibilities are

$$16 + 4 + 4, 16 + 4 + 1 + 1 + 1 + 1, \ldots, \underbrace{1 + \cdots + 1}_{24}$$

[1]The proof for the statement that if G is finite and $\operatorname{char} k$ divides $|G|$, then kG is not semisimple, is pretty much analogous to the case where G is infinite.

Because the last option is commutative, it cannot be correct. This was enough in the case of $G = S_3$, but here we need a better approach. By the Brandeis University notes on group representations[2], Theorem 1.18, the number of factors in the decomposition is equal to the number of conjugacy classes of S_4, which we know is equal to the number of cycle types of S_4. There are 5 cycle types of S_4: $(4), (3,1), (2,2), (2,1,1), (1,1,1,1)$. Hence the only possible decomposition is $9+9+4+1+1$, that is

$$\mathbb{C}[S_4] \cong M_3(\mathbb{C})^2 \times M_2(\mathbb{C}) \times \mathbb{C}^2$$

Ex. 3: Let A be a k-algebra. We will show that A is a finite-dimensional central simple k-algebra if and only if there exists a k-algebra B such that $A \otimes_k B \cong M_n(k)$ as k-algebras for some $n \in \mathbb{N}$.

- ($\implies$:) By a Proposition from the lectures, we have $A \otimes A^{\mathrm{op}} \cong M_n(k)$ for $n = [A : k]$. Simply take $B = A^{\mathrm{op}}$.
- ($\impliedby$:) Suppose for contradiction that A is not simple and take a proper ideal $I \lhd A$. Then $I \otimes B \lhd A \otimes B$ and is therefore isomorphic to some $J \lhd M_n(k)$. We know that all ideals of the matrix ring are of the form $M_n(N)$ for some $N \lhd k$. But k is a field and has no proper ideals, hence either $J \cong M_n(k)$ or $J \cong (0)$. Both cases lead to a contradiction, so A must be simple. Notice that the symmetry argument yields that B must also necessarily be simple. Then

  $$Z(A \otimes B) \cong Z(A) \otimes Z(B) \cong Z(M_n(k)) \cong k$$

  where $Z(A)$ and $Z(B)$ are both finite dimensional algebras that contain k. Hence by dimension count $Z(A) \cong k$, that is, A is central.

Ex. 4: Let D_1 and D_2 be finite-dimensional division k-algebra. Let us show that $D_1 \otimes_k D_2$ is a division ring if $\dim_k(D_1)$ and $\dim_k(D_2)$ are coprime.

We will mimic the solution of a similar exercise from tutorials, but adjust for the fact that D_1 and D_2 are not necessarily central. Namely, since D_1 and D_2 are division algebras and hence simple, they are central simple division algebras over $Z_1 = Z(D_1)$ and $Z_2 = Z(D_2)$, respectively. Tensoring clearly produces a $(Z_1 \otimes Z_2)$-algebra $D_1 \otimes D_2$, where by examining simple tensors we notice that $Z(D_1 \otimes D_2) = Z_1 \otimes Z_2$. By Wedderburn's Structure Theorem, we have that $D_1 \otimes D_2 \cong M_n(D_3)$. Clearly, $Z(D_3) = Z_1 \otimes Z_2$. Now denote $d_i = \deg_{Z_i} D_i$, $z_i = \deg_k Z_i$, and $d_3 = \deg_{Z_1 \otimes Z_2} D_3$ and get the equation

$$d_1 z_1 d_2 z_2 = n d_3 z_1 z_2$$

from which immediately follows

$$d_1 d_2 = n d_3 \tag{1}$$

where we have eliminated the degrees of the centers. Since $d_1 z_1$ and $d_2 z_2$ are coprime, necessarily d_1 and d_2 are coprime as well, and we will prove that $n = 1$ by proving that n divides both degrees.

We consider the ring $D_1 \otimes D_2 \otimes D_1^{\mathrm{op}}$ and see

$$D_1 \otimes D_1^{\mathrm{op}} \cong M_{d_1^2}(Z_1) \implies D_1 \otimes D_2 \otimes D_1^{\mathrm{op}} \cong M_{d_1^2}(Z_1 \otimes D_2) \cong M_n(D_3 \otimes D_1^{\mathrm{op}})$$

so we get

$$D_3 \otimes D_1^{\mathrm{op}} \cong M_{n_2}(Z_1 \otimes D_2) \cong M_{n_2}(D_2) \quad \text{as } Z_1 \otimes Z_2\text{-algebras}$$

and similarly for $D_1 \otimes D_2 \otimes D_2^{\mathrm{op}}$

$$D_3 \otimes D_1^{\mathrm{op}} \cong M_{n_1}(Z_2 \otimes D_1) \cong M_{n_1}(D_1) \quad \text{as } Z_1 \otimes Z_2\text{-algebras}$$

[2] `http://people.brandeis.edu/~igusa/Math101bS07/Math101b_notesD1a.pdf`, the statements of the two lemmas that prove this are longer than their proofs.

which produces the following equations

$$z_1 z_2 d_3 d_1 = n_2 z_1 z_2 d_2$$
$$z_1 z_2 d_3 d_2 = n_1 z_1 z_2 d_1$$

where we can again cancel the degrees of the centers. We get

$$d_3 d_1 = n_2 d_2$$
$$d_3 d_2 = n_1 d_1$$

Then with the use of (1) we calculate

$$d_1^2 d_3 = n_2 d_1 d_2 = n_2 n d_3 \implies d_1^2 = n_2 n \implies n | d_1^2$$
$$d_2^2 d_3 = n_1 d_1 d_2 = n_1 n d_3 \implies d_2^2 = n_1 n \implies n | d_2^2$$

Since d_1 and d_2 are coprime, so are their squares, so $n = 1$ and $D_1 \otimes D_2 \cong D_3$.

Ex. 5: Let R be a local ring and $A \in M_n(R)$, where $a_{i,j}$ is invertible precisely when $i = j$, that is, on the diagonal. We will show that A is invertible.

We will actually prove a seemingly stronger statement, that for a local ring R we have that $A \in M_n(R)$ is invertible precisely when $\overline{A} \in M_n(R/\operatorname{rad}(R))$ is invertible.

- ($\Longleftarrow$:) Since R is local, $R^{-1} = R \setminus \operatorname{rad} R$, so if $\det(\overline{A}) \neq 0 \in R/\operatorname{rad}(R)$, then $\det(A) \in R^{-1}$, since $\det \overline{A} = \overline{\det A}$.
- ($\Longrightarrow$:) Similarly, $A \in M_n(R)$ is invertible precisely when $\det A \in R^{-1} = R \setminus \operatorname{rad} R$. Then we simply have $\det \overline{A} = \overline{\det A} \neq 0 \in R \setminus \operatorname{rad} R$. Hence $\overline{A}$ is invertible.

We now return back to the exercise. If A is of the following form

$$A = \begin{bmatrix} R^{-1} & \cdots & \operatorname{rad} R \\ \vdots & \ddots & \vdots \\ \operatorname{rad} R & \cdots & R^{-1} \end{bmatrix}$$

then $\overline{A}$ is of the form

$$A = \begin{bmatrix} R/\operatorname{rad} R & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & R/\operatorname{rad} R \end{bmatrix}$$

where the diagonal elements are non-zero, which is clearly invertible, as $R/\operatorname{rad} R$ is a division ring. Hence A is invertible.

Ex. 6: Let A be a k-algebra and M an A-bimodule. We equip the set $A \times M$ with componentwise addition, scalar multiplication, and the following multiplication

$$(a, m) \cdot (b, n) = (ab, an + mb).$$

(a) Show that $A_M = A \times M$ is a k-algebra for the above operations.

Since addition and scalar multiplication clearly satisfy the axioms, we focus on multiplication.

- *associativity*: We merely calculate

$$((a, m)(b, n))\,(c, o) = (ab, an + mb)(c, o) = (abc, abo + (an + mb)c)$$

and

$$(a, m)\,((b, n)(c, o)) = (a, m)(bc, bo + nc) = (abc, a(bo + nc) + mbc)$$

which are equal expressions since M is a module.

- *distributivity*: Holds since addition and scalar multiplication are defined componentwise. For example, we have

$$\begin{aligned}(a,m)\cdot((b,n)+(c,o)) &= (a,m)\cdot(b+c,n+o)\\ &= (a(b+c),a(n+o)+m(b+c))\\ &= (ab+ac,an+ao+mb+mc)\\ &= (ab,an+mb)+(ac,ao+mc)\\ &= (a,m)\cdot(b,n)+(a,m)\cdot(c,o)\end{aligned}$$

  and similarly for scalar multiplication and having addition on the other side.

(b) Show that A is a PI-algebra $\iff$ A_M is a PI-algebra.

- ($\Longleftarrow$): We can embed A into A_M by identifying $A \longleftrightarrow A\times\{0\}$, since the operations on A_M on the first component are exactly the operations on A. Then clearly any polynomial identity on A_M will be a polynomial identity on A via the above identification.
- ($\Longrightarrow$): Let f be a non-zero polynomial identity on A. If we instead apply it to elements of A_M, we get $f((a,m))=(0,n)$ where we do not really know what is the second component. But, by the way multiplication is defined on A_M, we see that

$$f((a,m))\cdot f((a,m)) = (0,n)\cdot(0,n) = (0,0n+n0) = (0,0)$$

  hence f^2 defines a non-trivial polynomial identity on A_M.

Ex. 7: Let A be a k-algebra with $\operatorname{char}(k)=0$ and let $e,e',e''\in A$ be idempotents. Assume $e+e'+e''=\lambda\cdot 1$ holds for some $\lambda\in k$.

(a) Show that $\lambda\in\left\{0,1,2,3,\frac{3}{2}\right\}$.

(b) Show that e, e', e'' commute if $\lambda\in\{0,1,2,3\}$.

First notice that by taking e, e' and e'' to be trivial idempotents we easily obtain $\lambda\in\{0,1,2,3\}$. Next notice, that the only way to get $\lambda=0$ is by all three idempotents being 0. Indeed, suppose $e''\neq 0$. Then $e''=-e-e'$, and since a negation of an idempotent is not one, both e and e'' must also be different from 0. But we see that $-e-e'$ is an idempotent, so

$$-e-e' = (e+e')^2 = e^2+ee'+e'e+e'^2 = e+e'+ee'+e'e$$

and we get

$$2e'' = ee'+e'e$$

Input this into the first formula multiplied by 2 and we get

$$2e+2e'+ee'+e'e=0 \implies e+e'+(e+e')^2=0$$

and obtain

$$(e+e')(1+e+e')=0$$

but $1-e''=1+e+e'$, so $e''=e+e'=-e-e'$, hence $e''=0$. (This also proves that if $\lambda=0$, the idempotents commute, as they are all 0.)

Recall that in a finite dimensional k-algebra, a sum of idempotents is an idempotent precisely when the terms of the sum are pairwise orthogonal (since $\operatorname{char} k=0$). Indeed, let us prove this for a sum of 2 idempotents. Assume $e_1+e_2=e_3$ where all e_i are idempotent. Then

$$\begin{aligned}(e_1+e_2)^2 &= e_3^2\\ e_1+e_2+e_1e_2+e_2e_1 &= e_3 = e_3\\ e_1e_2+e_2e_1 &= 0\end{aligned}$$

We multiply the result by e_1 from the left and the right and get

$$2e_1e_2e_1 = 0$$

but $e_1e_2 = -e_2e_1$, so we get

$$e_1e_2e_1 = -e_1^2e_2 = -e_1e_2 = 0$$

This can be generalized to an arbitrary finite number of idempotents using induction.

Assume now that $\lambda \in \{0, 1, 2, 3\}$. We separate cases

- $\underline{e + e' + e'' = 0:}$ Since 0 is trivially an idempotent, e, e', e'' must be pairwise orthogonal, in particular they pairwise commute.
- $\underline{e + e' + e'' = 1:}$ It follows that
$$1 - e'' = e + e'$$
which is an idempotent. Hence e and e' are orthogonal and in particular commute. Since there is nothing special about e'', we repeat the argument for the other two possibilities and obtain that all e, e', e'' pairwise commute.
- $\underline{e + e' + e'' = 2:}$ It follows that
$$e'' = (1 - e) + (1 - e')$$
so $(1 - e)$ and $(1 - e')$ are pairwise orthogonal and hence commute. We get that e and e' must also commute, since
$$\begin{aligned}(1 - e)(1 - e') &= (1 - e')(1 - e)\\ 1 - e - e' - ee' &= 1 - e - e' - e'e\\ ee' &= e'e\end{aligned}$$
We repeat this for other possibilities and obtain that all e, e', e'' pairwise commute.
- $\underline{e + e' + e'' = 3:}$ It follows that
$$e'' = 1 + (1 - e) + (1 - e')$$
from which we again get that $(1 - e)$ and $(1 - e')$ commute. Proceed as in the above case.

This proves part (b), but what remains to be seen is that the only other possibility for λ is $\frac{3}{2}$. Notice that it is enough to show that $\lambda = e + e' + e''$ satisfies the following polynomial equation

$$x(x-1)(x-2)(x-3)(x-\frac{3}{2}) = x^5 - \frac{15}{2}x^4 + 20x^3 - \frac{45}{2}x^2 + 9x = 0$$

where e, e', e'' are assumed to be non-commutative variables. We will solve this problem using the non-commutative Gröbner basis algorithm in `Mathematica`. The full notebook will be available as an attachment to this document named `neka_hw6_ex7.nb`.

Let us examine the solution. We first import the `Mathematica` module `NC` for performing non-commutative computation:[3]

```
<< NC`
```

We then enable computation with non-commutative objects and Gröbner basis calculation:

```
<< NCAlgebra`
<< NCGBX`
```

Next we need to define our monomial order. We will use `l, x, y, z` to stand for λ, e, e', e'', respectively. It is crucial to put `l` in the first place in the order, as this will yield an equation only containing `l` in the end. Otherwise, the order does not really matter, so we define our monomial order as follows:

[3]This module is available on `Github` at `https://github.com/NCAlgebra/NC`. To install simply run `git clone <url>` somewhere in your `Mathematica` path.

```
SetMonomialOrder[l, {x, y, z}];
```

In the notebook we also print it out to be certain. In the next step we define the system of equations we are actually trying to solve. Indeed, our problem can be more precisely encoded in the following system of equations

$$\begin{aligned} e + e' + e'' &= \lambda \\ e^2 &= e \\ e'^2 &= e' \\ e''^2 &= e'' \\ \lambda e &= e\lambda \\ \lambda e' &= e'\lambda \\ \lambda e'' &= e''\lambda \end{aligned}$$

where we consider λ as just another variable with the special property of commuting with all the other variables. This produces an ideal that is encoded with the above relations as:

```
rels = {x + y + z - l, x^2 - x, y^2 - y, z^2 - z, lx - xl, ly - yl, lz - zl}
```

What remains is to run the algorithm and display the results in a readable fashion:

```
ColumnForm[NCMakeGB[rels, 10]]
```

The very last line of the output gives us that λ is in fact subject to the relation

$$\lambda^5 = -9\lambda + \frac{45}{2}\lambda^2 - 20\lambda + \frac{15}{2}\lambda^4$$

which is exactly what we set out to prove.

Ex. 8: Find a polynomial identity of $M_n(\mathbb{Q})$ for $n = 2, 3$ with the least monomials. What about for general n?

Or

Find a polynomial identity in two variables of $M_n(\mathbb{Q})$ for $n = 2, 3$ with the minimal degree. What about for general n?

We try to solve the second option. By a Lemma from the lectures we know that $M_n(\mathbb{Q})$ has no non-zero polynomial identity of degree less than $2n$. From the proof it is evident that this also holds for multilinear identities, in particular for those in two variables.

Now recall the Amitsur-Levitzki Theorem, which gives us that the standard polynomial s_{2n} is an identity for $M_n(\mathbb{Q})$. The only issue is that s_{2n} is a multilinear identity in $2n$ variables. However, this can easily be fixed by defining

$$f_n(X, Y) = s_{2n}(\underbrace{X, \ldots, X}_{n}, \underbrace{Y, \ldots, Y}_{n})$$

which is now an identity in two variables that by the above must have minimal degree $2n$.

In the particular case of $n = 2, 3$ this gives us

$$f_2(X, Y) = s_4(X, X, Y, Y)$$

and

$$f_3(X, Y) = s_6(X, X, X, Y, Y, Y)$$

respectively.

Ex. 9: I will describe some ways non-commutative algebra is important in general and try to provide examples, but mainly I will present how the topics from the course relate to my own research interests.

The short answer is that many of the objects that we study in other mathematical fields that are more directly applicable to, e.g., physics are algebraically rings or even algebras, most notably a matrix *ring*, the *algebra* of continuous functions etc., which are very often non-commutative. It thus makes sense to understand such objects purely algebraically, which can then lead to understanding them better in other contexts, e.g., geometrically or analytically.

Let us look at some examples showing the importance of non-commutative algebra in other fields.

- One of the most important tools in the study of manifolds is (co)homology. In the `Algebraic Topology 1` class we looked at homology from the axiomatic perspective (as opposed to `Algebraic Topology 2` which was focused more on calculations) and thus defined a homology theory h_* as a collection of functors $h_n \colon \mathbf{Top^2} \to R\text{−}\mathbf{Mod}$. We normally look at the case where $R = \mathbb{Z}$ and consider Abelian groups, but this is not always the case. As we have seen in one of the homeworks, some key theorems such as the Universal Coefficient Theorem depend greatly on the structure of R. It is therefore important to consider algebraic properties of R-modules when studying manifolds with different homology theories. In the homework it turned out that R had to be principal, but one can imagine even greater pathologies arise when we consider modules over non-commutative rings.

- While researching sources for the first exercise of Homework 3 I stumbled upon a `mathoverflow`[4] post which essentially stated that every simple C^*-algebra in which $[x, y]^2$ is central for all x, y is isomorphic to $M_n(\mathbb{C})$ for $n = 1, 2$. Indeed, the way I initially approached the exercise was by substituting z, w with x, y, respectively, thus obtaining

  $$[x, y]^2 \in k = Z(A)$$

  We see that the statement from the field of functional analysis is further generalized, or rather more easily proved, using merely algebraic means and our notion of the central simple algebra. But, as central simple algebras seem too abstract a concept, the notion of a C^*-algebra arises naturally in physics both in classical and quantum mechanics. We are thus able to use the knowledge we obtained in the chapter discussing central simple algebras to assist the general understanding of a physical concept, however slightly. Moreover, the accepted answer in the post mentioned above used PI-algebras to prove their claim, which is a concept we also considered in the last chapter of the course.

Let us now look at the way I have used the topics from the course to further my own mathematical interests. One of the main fields of study I am interested in is cryptography, and as I have found out in the past months, contemporary cryptography is largely based on non-commutative algebra. To give a few examples:

- We have studied the notion of a quaternion algebra quite a bit during the course, especially during tutorials, and while researching contemporary cryptography I found an article by Bagheri K. et al. titled "A Non-commutative Cryptosystem Based on Quaternion Algebras"[5] discussing using quaternion algebras to construct a modern lattice-based cryptosystem.

- While computationally inefficient, the Gröbner bases are still a powerful method of analysing algebraic weaknesses of a cryptosystem, historically mainly used against block ciphers. With new cryptosystems being increasingly non-commutative in nature, developing a somewhat efficient Gröbner bases algorithm operating on non-commutative polynomials is paramount. Great work has already been done by the `NCAlgebra` project[6] which I already used in my programmatic solution of exercise 7, and similar functionality is available in some other frameworks for mathematical computation.

[4] https://mathoverflow.net/questions/299784/simple-c-algebras-whose-all-commutator-elements-have-scalar-square
[5] https://arxiv.org/abs/1709.02079
[6] https://github.com/NCAlgebra/NC

- There are many more examples of using non-commutative algebra in modern cryptography using precisely the concepts we have studied in the course, mainly using either non-commutative polynomials or central simple algebras, I have even found one using non-commutative group rings, and I do not wish to be too long.

I hope this exposition ties the course sufficiently to the world of the "usable", even though the concepts are interesting on their own.