Noncommutative algebra - 1$^{\text{st}}$ homework

Benjamin Benčina, 27192018

6. november 2020

<u>Ex. 1:</u> Let k be a field and A a finite dimensional k-algebra. Let us show that every element of A is either a unit or a zero-divisor.

Consider the following two maps

$$\begin{aligned} L_a \in \operatorname{End}_k(A): &\quad x \mapsto ax \\ R_a \in \operatorname{End}_k(A): &\quad x \mapsto xa \end{aligned}$$

Since k is a field, A is in fact a finite dimensional vector space over k. Linear maps L_a and R_a are therefore surjective iff they are injective. Clearly L_a is injective precisely when $a \in A$ is not a left zero-divisor (look at the kernel). Let us now prove that L_a is surjective precisely when a is right invertible. Both implications are clear, indeed, we have

- ($\implies$): For every $x \in A$ there exists $y \in A$ such that $ay = x$. In particular, for $x = 1$ there exist $y \in A$ such that $ay = 1$.
- ($\impliedby$): There exists $b \in A$ such that $ab = 1$. Clearly we have that for every $x \in A$, $bx \mapsto abx = x$.

Similarly we prove analogue statements for R_a with left $\longleftrightarrow$ right.

Suppose now that $a \in A$ is not a zero-divisor. This by definition means that it is not a left zero-divisor and that it is not a right zero-divisor. By the above, a is left and right invertible and therefore invertible. Clearly, no zero-divisor can be invertible.

<u>Ex. 2:</u> Let M be an artinian and noetherian R-module and $\varphi \in \operatorname{End}_R(M)$ We will show that there exists $n \in \mathbb{N}$ such that $M = \operatorname{im}(\varphi^n) \oplus \ker(\varphi^n)$.

We first notice that for every $n \in \mathbb{N}$ we have $\ker \varphi^n \subseteq \ker \varphi^{n+1}$ and $\operatorname{im} \varphi^{n+1} \subseteq \operatorname{im} \varphi^n$. Also note that since φ is linear, $\ker \varphi^n$ and $\operatorname{im} \varphi^n$ are submodules in M for every $n \in \mathbb{N}$.

Now consider the following two chains

$$\begin{gathered} \ker \varphi \leq \ker \varphi^2 \leq \ker \varphi^3 \leq \cdots \\ \operatorname{im} \varphi \geq \operatorname{im} \varphi^2 \geq \operatorname{im} \varphi^3 \geq \cdots \end{gathered}$$

Since M is noetherian, there exists $k \in \mathbb{N}$ such that $\ker \varphi^k = \ker \varphi^{k+1} = \cdots$, and since M is artinian, there exists $l \in \mathbb{N}$ such that $\operatorname{im} \varphi^l = \operatorname{im} \varphi^{l+1} = \cdots$; denote $N = \max\{k, l\}$. We will prove that $M = \operatorname{im} \varphi^N \oplus \ker \varphi^N$.

- Take $x \in \ker \varphi^N \cap \operatorname{im} \varphi^N$, that is $\varphi^N x = 0$ and there exists $y \in M$ such that $\varphi^N y = x$. It follows that $\varphi^{2N} y = 0$, therefore $y \in \ker \varphi^{2N} = \ker \varphi^N$, so we have $x = \varphi^N y = 0$ and the intersection is trivial.
- Take $x \in M$. Since $\operatorname{im} \varphi^N = \operatorname{im} \varphi^{2N}$, there exists $y \in M$ such that $\varphi^N x = \varphi^{2N} y$. Then we can decompose $x = (x - \varphi^N y) + \varphi^N y$, where the first term is in $\ker \varphi^N$ and the second term is in $\operatorname{im} \varphi^N$.

Ex. 3: We will show that a module M is semisimple iff every one of its cyclic submodules is semisimple.

The implication from left to right is trivial. Every submodule of a semisimple module is semisimple, in particular every cyclic submodule.

For the converse notice that every module can be written as a sum of its cyclic submodules, that is

$$M = \Sigma_{m \in M} Rm$$

where note that the above sum is in general not direct. By assumption, every cyclic submodule is semisimple and can therefore be written as a direct sum of simple submodules, that is for every $m \in M$ we have

$$Rm = \bigoplus_{i \in I_m} N_i^m$$

If follows now that M is a sum of simple modules (not necessarily direct). By a proposition from the lectures, M is semisimple.

Ex. 4: Let R be a ring with unity. We shall compute the Jacobson radical J of $U_n(R)$ the ring of all upper triangular $n \times n$ matrices over R (not unitary matrices).

As a first step, we simply guess the Jacobson radical:

$$J = \begin{bmatrix} \operatorname{rad} R & R & \dots & R \\ & \operatorname{rad} R & \dots & R \\ & & \ddots & \vdots \\ & & & \operatorname{rad} R \end{bmatrix}$$

It is fairly easy to see that J is both a left and a right ideal, which follows from the fact, that $\operatorname{rad} R$ is a two-sided ideal, and the properties of matrix multiplication. Furthermore, if $J \subseteq \operatorname{rad} U_n(R)$, it follows that

$$\operatorname{rad}(U_n(R))/J = \operatorname{rad}(U_n(R)/J) \cong \operatorname{rad}(R/\operatorname{rad} R \times \dots \times R/\operatorname{rad} R) \cong (0)$$

since $R/\operatorname{rad} R$ is J-semisimple. Clearly then $J = \operatorname{rad} U_n(R)$.

As we see now, we have to prove $J \subseteq \operatorname{rad} U_n(R)$. Concretely, we will prove that for every left maximal ideal $M < U_n(R)$ we have $J \subseteq M$. We observe that for every $i = 1, \dots, n$ matrices in $U_n(R)$ that have elements ranging over the entire R all but on the i-th diagonal place, where they are ranging over some maximal left ideal $M < R$, form a left ideal (again apparent from matrix multiplication) which is obviously maximal. Moreover, if we put a maximal left ideal anywhere else but on the diagonal, by the properties of matrix multiplication, we get the entire $U_n(R)$ back. Of course any left ideal that has left ideals of R on more than one place is contained in one of the above ideals (by maximality of left ideals M). Therefore, every maximal left ideal is of the above form, but J is clearly contained in all of them, since all of its diagonal elements are ranging over $\operatorname{rad} R$ (which is by definition contained in all maximal left ideals of R).

Ex. 5: Let R be an artinian ring and G a finite group. Let us show that the group ring RG is a semisimple ring iff R is a semisimple and $|G|$ is invertible in R.

- ($\Longleftarrow$): This direction seems similar to the formulation of Maschke's theorem with the complication that we have merely an artinian ring, not a field. We nonetheless try and follow the proof as much as possible. Indeed, let $M \leq RG$ be an RG-submodule. We're proving that M has a complement in RG. Since R is semisimple, these exists a projection map of R-modules $f\colon RG \to M$ ($f|_M$ is the identity map). We construct the following "averaging"map $g\colon RG \to RG$ with

$$g(x) = \frac{1}{|G|} \Sigma_{\sigma \in G} \sigma^{-1} f \sigma x$$

and claim that g is an RG-linear projection map with respect to M (here $\frac{1}{|G|}$ denotes the inverse of $|G|$). Indeed, with the same steps as at the lectures, we prove that for every $x \in RG$ we have $g(x) \in M$, for every $x \in M \leq RG$ we have $g(x) = x$ (both of these are trivial to see, since f is a projection with respect to M and R-linear), and that (since addition is trivial) that for every $\tau \in G$ and $x \in RG$ we have $g(\tau x) = \tau g(x)$ (we merely switch around group elements). It follows that $RG = M \oplus \ker g$ and by a proposition from the lectures (every submodule is a direct summand), RG is semisimple.

- ($\Longrightarrow$): Suppose that RG is a semisimple ring (that is, semisimple as an RG-module). We first show that R is semisimple.

  In the standard way we embed R into RG as a submodule via the identification $R \longleftrightarrow R(\Sigma_{\sigma\in G}\sigma)$. Indeed, R is now a RG submodule; it is clearly closed for addition and multiplication with finite sums from RG, since we chose $\Sigma_{\sigma\in G}\sigma$ as the generator and for every $\tau \in G$ we have $\tau\Sigma_{\sigma\in G}\sigma = \Sigma_{\sigma\in G}\sigma$. It follows that every R-submodule of R will be an RG-submodule of R (under identification) and thus R is semisimple too.

  Now consider the augmentation map $\varepsilon\colon RG \to R$ (given by the trivial action of G on R) defined by
  $$\Sigma_{\sigma\in G} r_\sigma \sigma \mapsto \Sigma_{\sigma\in G} r_\sigma$$
  and let us look at $I = \ker\varepsilon$ an RG-submodule of RG. Since RG is semisimple it satisfies the complement property, so there exists a (one-sided) ideal C of RG such that $RG = I \oplus C$. Let us decompose the multiplicative neutral element of R under identification as $1 = e + c$ with $e \in I$ and $c \in C$ in a unique way. Squaring the expression we see $e^2 = e$. Since our augmentation map was given by the trivial action of G on R, G acts trivially on RG/C, so $e\sigma = e$ for each $\sigma \in G$. It follows that $e = t\Sigma_{\sigma\in G}\sigma$ for some $t \in R$. However e is an idempotent, so from a calculation from the tutorials it follows that
  $$e^2 = |G|t^2\Sigma_{\sigma\in G}\sigma = t\Sigma_{\sigma\in G}\sigma = e$$
  Comparing coefficients (remember, G is a basis for RG) we get $|G|t^2 = t$ at the unit of the group G. Furthermore, there is no $r \in R$ such that $rt = tr = 0$. Indeed, e acts as the identity on the RG-module R, and if $rt = 0$ in R then $e = t\Sigma_{\sigma\in G}\sigma$ annihilates r in the natural action of RG on R, same for $tr = 0$. Hence we're justified in cancelling the extra t in the above equation and we get that $|G|t = 1$ in R, hence $|G|$ is invertable ($|G|$ obviously commutes with t as a sum of $|G|$-many 1s).