Problem Set 2
Algebra III

Bennett Rennier
bennett@brennier.com

Ex 1. Assume that K is a finite field extension of k, where $n = [K : k]$, and a an element of K. Let $f : K \to \mathrm{End}_k(K) = \mathrm{M}_n(k)$ (the latter with respect to a fixed k-basis of K) be the canonical representation of the k-algebra K.

a) Show that the minimal polynomial of a over k (in the sense of field theory) is equal to the minimal polynomial of the matrix $f(a)$ (in the sense of linear algebra).

b) Now assume additionally that K is Galois over k with Galois group $G = \{g_1, g_2, \ldots, g_n\}$, and that $K = k(a)$. Prove that $T_{K|k}(a) = g_1(a) + \cdots + g_n(a)$ and that $N_{K|k}(a) = g_1(a) \cdots g_n(a)$.

Proof.

a) First, let $p_f(x)$ be the the minimal polynomial of a in the field theory sense and let $p_\ell(x)$ be the minimal polynomial of $f(a) = \lambda_a$ as a matrix representing left multiplication by a. Let $p_\ell(x) = \sum_{i=1}^n k_i x^i$. Then by definition we have that $p_\ell(\lambda_a) = \sum_{i=1}^n k_i \lambda_a^i = 0$. This means that if we evaluate this linear map at 1 we get

$$0 = \left(\sum_{i=1}^n k_i \lambda_a^i\right)(1) = \sum_{i=1}^n k_i \lambda_a^i(1) = \sum_{i=1}^n k_i a^i = p_\ell(a).$$

Similarly, if we have that $p_f(x) = \sum_{i=1}^m k_i x^i$, we see that for every $k' \in K$

$$p_f(\lambda_a)(k') = \left(\sum_{i=1}^m k_i \lambda_a^i\right)(k') = \sum_{i=1}^n k_i \lambda_a^i(k') = \sum_{i=1}^n k_i a^i k' = \left(\sum_{i=1}^n k_i a_i\right) k' = p_f(a) \cdot k' = 0 \cdot k' = 0$$

which proves that $p_f(\lambda_a)$ is the zero map. Since the sets $\{p \in k[x] : p(a) = 0\}$ and $\{p \in k[x] : p(\lambda_a) = 0\}$ are both ideals generated by p_f and p_ℓ respectively and we know that both polynomials belong to both of the ideals, we get that p_f divides p_ℓ and p_ℓ divides p_f. This proves that one must be some multiple of the other, but since they both have leading coeffecients of 1 by definition, we have that $p_\ell = p_f$ as desired.

b) Let $p(x)$ be the minimal polynomial of a in K over k and let $R = \{a, r_2, \ldots, r_n\}$ be the roots of $p(x)$. As Galois extensions are separable, we have that $p(x) = \prod_{r \in R}(x - r)$. Since the Galois group acts transitively on the roots R, we can assume without loss of generality that $g_1(a) = a$ and that $g_i(a) = r_i$. This means that $p(x) = \prod_{g_i \in G}(x - g_i(a))$. By part (a), $p(x)$ is also the minimal polynomial of the matrix λ_a. Thus, the roots of this polynomial are eigenvalues of λ_a. Since there are n distinct roots, this means λ_a is diagonalizable with the eigenvalues $\{g_i(a)\}_{i \le n}$ as its diagonal entries. Thus,

$$T_{K_k}(a) = \mathrm{Tr}(\lambda_a) = g_1(a) + \cdots + g_n(a)$$

and

$$N_{K_k}(a) = \det(\lambda_a) = g_1(a) \cdots g_n(a)$$

as desired. □

Ex 2.

a) If $f : R \to S$ is an isomorphism between two finite-dimensional k-algebras, show that $N_{R|k}(x) = N_{S|k}(f(x))$ and $T_{R|k}(x) = T_{S|k}(f(x))$ for all $x \in R$.

b) Assume that $K|k$ is a field extension, S is a finite-dimensional K-algebra and R is a k-algebra which is also a subring of S. Assume further that there exists a k-basis of R which is also a K-basis of S. Show that $N_{R|k}(x) = N_{S|K}(x)$ and $T_{R|k}(x) = T_{S|K}(x)$ for all $x \in R$.

c) If R is a quaternion algebra over k (where $\mathrm{char}(k) \neq 2$), find and prove a relation between the quaternion norm $N(x)$ and the canonical norm $N_{R|k}(x)$ for $x \in R$.

Proof.

a) Let $\{e_1, \ldots, e_n\}$ be a basis of R. Since f is an isomorphism, we know that $\{f(e_1), \ldots, f(e_n)\}$ is a basis of S. Let $x \in R$ and let $xe_j = \sum_{i=1}^n k_{ij} e_i$ for $1 \leq j \leq n$. Since means that with respect to the basis $\{e_1, \ldots, e_n\}$, the linear map $\lambda_x : R \to R$ has matrix form $(k_{ij})_{i,j \leq n}$. We also see that

$$f(x)f(e_j) = f(xe_j) = f\left(\sum_{i=1}^n k_{ij} e_i\right) = \sum_{i=1}^n f(k_{ij}) f(e_i) = \sum_{i=1}^n k_{ij} f(e_i)$$

which means that with respect to basis $\{f(e_1), \ldots, f(e_n)\}$, the linear map $\lambda_{f(x)} : S \to S$ has matrix form $(k_{ij})_{i,j \leq n}$ as well. Thus

$$N_{R|k}(x) = \det(\lambda_x) = \det(\lambda_{f(x)}) = N_{S|k}(x),$$
$$T_{R|k}(x) = \mathrm{Tr}(\lambda_x) = \mathrm{Tr}(\lambda_{f(x)}) = T_{S|k}(x)$$

as desired.

b) Let $\{e_1, \ldots, e_n\}$ be a k-basis of R that is also a K-basis of S. let $x \in R$ and let $xe_j = \sum_{i=1}^n k_{ij} e_i$ for $1 \leq j \leq n$. Thus, with respect to the basis $\{e_1, \ldots, e_n\}$, the linear map $\lambda_x : R \to R$ has matrix form $(k_{ij})_{i,j \leq n}$. We note that since R is a subring of S, we have that $x \in S$. By assumption, S has the same basis, so it is still true that $xe_j = \sum_{i=1}^n k_{ij} e_i$, this time considering $k_{ij} \in K$. This means that the map $\lambda_x : S \to S$ where x is considered an element of S can be represented by the same matrix $(k_{ij})_{i,j \leq n}$. Thus, we have that

$$N_{R|k}(x) = \det((k_{ij})_{i,j \leq n}) = N_{S|K}(x),$$
$$T_{R|k}(x) = \mathrm{Tr}((k_{ij})_{i,j \leq n}) = T_{S|K}(x)$$

as desired.

c) I'm not entirely sure how to do this. If R is the quaternion algebra $(a, b)/k$, we will probably need to consider R as a $K = k(\sqrt{a}, \sqrt{b})$ algebra with the same basis. I don't know how to relate this to the usual quaternion norm $N(x)$ for any field k, though. □

Ex 3. Let V be a k-vector space with a countable infinite basis. Set $R = \mathrm{End}(V)$. As you were supposed to show in Exercise 2(c) of Homework 1, $I = \{f \in R : \mathrm{rank}(f) < \infty\}$ is a nontrivial proper two-sided ideal of R.

a) If f is in $R \setminus I$, show that there exist elements g and h in R with $gfh = \mathrm{Id}_V$.

b) Deduce that the quotient ring R/I is simple. Remark: R/I is an example of a simple ring which is not semi-simple.

Proof.

a) Let $\{e_\alpha\}_{\alpha\in\mathbb{N}}$ be a basis of $f(V)$. We know that we can use $\mathbb{N}$ as the indexing set, as since $f \notin I$, the image has infinite dimension, and since $f(V) \subseteq V$, $f(V)$ must be countable as a subspace of a countable vector space. Since we can always extend bases, there is a basis $\{d_\beta\}_{\beta\in\mathbb{N}}$ of V such that $\{e_\alpha\}_{\alpha\in\mathbb{N}} \subseteq \{d_\beta\}_{\beta\in\mathbb{N}}$.

   Now, define $g : V \to V$ by $g(e_i) = d_i$ for $i \in \mathbb{N}$ and $g(d_j) = 0$ for $d_j \notin \{e_\alpha\}_{\alpha\in\mathbb{N}}$. Thus, we have that $\mathrm{im}(g \circ f)$ contains every d_i, so $g \circ f$ is surjective. By the previous homework, every such surjective map has a left inverse, so there is an h such that $g \circ f \circ h = \mathrm{Id}_V$ as desired.

b) Let J be a nonzero ideal of R/I and let $f + I \in J$ be a nonzero element of J. Specifically, this means that $f + I \neq I$, meaning $f \notin I$. Thus, by part (a), there are maps $g, h \in R$ such that $(g + I)(f + I)(h + I) = gfh + I = \mathrm{Id}_V + I \in J$. Since J contains the 1 in our ring R/I, it must be that $J = R/I$. Thus, the only ideals of R/I are $\{0\}$ and R/I itself, proving R/I is simple. $\square$

Ex 4. Suppose that R is a commutative ring, that I and J are ideals of R, and that the quotients R/I and R/J are isomorphic R-modules. Prove that $I = J$ (equal, not just isomorphic!). Point out where your argument does not work if R is not commutative and I and J are just left ideals of R.

Proof. Let $r \in \mathrm{Ann}_R(R/J)$. In particular, we have that $0 + J = r \cdot (1 + J) = r \cdot 1 + J = r + J$. Thus $r \in J$, proving that $\mathrm{Ann}_R(R/J) \subseteq J$. Since $j \cdot (x + J) = jx + J = J = 0 + J$ (note, here we use that J is a right ideal), we have that $J \subseteq \mathrm{Ann}_R(R/J)$ as well. Thus, $J = \mathrm{Ann}_R(R/J)$ and by similar argument $I = \mathrm{Ann}_R(R/I)$. Let $\phi : R/I \to R/J$ be an isomorphism. Then if $r \in \mathrm{Ann}_R(R/I)$ we have

$$0 + J = \phi(0 + I) = \phi(r \cdot (x + I)) = r \cdot \phi(x + I)$$

proving that $r \in \mathrm{Ann}_R(R/J)$. By similar argument with ϕ^{-1}, we see that the two annihilators are equal. This means that

$$I = \mathrm{Ann}_R(R/I) = \mathrm{Ann}_R(R/J) = J$$

as desired. $\square$

Ex 5. Let $(M_i)_{i\in I}$ be a family of submodules of an R-module M. Denote by N_i the sum of all M_j for $j \in I \setminus \{i\}$. Suppose that M is the sum of all M_i.

a) Show that M is the direct sum of the M_i if and only if the intersection of M_i and N_i is trivial for all $i \in I$.

b) Give an example where $I = \{1, 2, 3\}$, $M = M_1 + M_2 + M_3$ and $M_1 \cap M_2 = M_2 \cap M_3 = M_3 \cap M_1 = \{0\}$, but where $M \neq M_1 \oplus M_2 \oplus M_3$.

Proof.

a) $\Longrightarrow$) Suppose $M = \oplus_{j\in I} M_j$ and let $n \in M_i \cap N_i$ for some $i \in I$. Since $n \in N_i = \sum_{j\neq i} M_j$, this means $n = \sum_{j\neq i} m_j$, where $m_j \in M_j$. M$_i$, we know that $-n \in M_i$. We can denote

$-n = m_i$ to emphasize that $m_i \in M_i$. With this, we have that

$$0 = n - n = n + (-n) = \sum_{j \neq i} m_j + m_i = \sum_{j \in I} m_j \in \bigoplus_{i \in I} M_i.$$

This means that $m_j = 0$ for all $j \in I$, and in particular that $m_i = (-n) = 0$, which means $n = 0$ as well. Since i was arbitrary, this proves that $M_i \cap N_i$ is trivial for all $i \in I$.

$\Longleftarrow$) Suppose that $\sum_{j \in I} m_j = 0$ where $m_j \in M_j$ and let i be any element of I. Then we have that $m_i \in M_i$ and that

$$m_i = -\sum_{j \neq i} m_j = \sum_{j \neq i} (-m_j) \in \sum_{j \neq i} M_j = N_i.$$

This means that $m_i \in M_i \cap N_i$. By assumption, this intersection is trivial, so it must be that $m_i = 0$. Since i was an arbitrary element of I, we have that $m_j = 0$ for all $j \in I$. This proves that $\sum_{j \in I} M_j = \oplus_{j \in I} M_j$ as desired.

b) Let $M = \mathbb{R}^2$ with standard basis $\{e_1, e_2\}$. Let $M_1 = \langle e_1 \rangle$, $M_2 = \langle e_2 \rangle$, and $M_3 = \langle e_1 + e_2 \rangle$ (i.e., the x-axis, the y-axis, and the line $x = y$ respectively). Since these are all subspaces of dimension 1 and their generators are pairwise linearly independent, we have that the intersection of any two of them is trivial. However, $M \neq M_1 \oplus M_2 \oplus M_3$ as $1 \cdot e_1 + 1 \cdot e_2 + (-1) \cdot (e_1 + e_2) = 0$. □

Ex 6. Let $f : N \to M$ and $f' : M \to N$ be two R-module homomorphisms satisfying $f'f = \mathrm{Id}_N$. Prove that M is the direct sum of $f(N)$ and $\ker(f')$.

Proof. Let $m \in M$. If $f'(m) = 0$, then we have that $m = 0 + m \in f(N) + \ker(f')$. Otherwise, $f'(m) \neq 0$. In this case, we have that

$$f'(m - f(f'(m))) = f'(m) - f'(f(f'(m))) = f'(m) - \mathrm{Id}_N(f'(m)) = f'(m) - f'(m) = 0,$$

which means $m - f(f'(m)) \in \ker(f')$. Thus, we have that $m = f(f'(m)) + (m - f(f'(m))) \in f(N) + \ker(f')$. This proves that $M = f(N) + \ker(f')$.

To prove that the sum is direct, let $m \in f(N) \cap \ker(f')$. This means that $f'(m) = 0$ and that there's some $n \in N$ such that $m = f(n)$. This means that

$$n = \mathrm{Id}_N(n) = f'(f(n)) = f'(m) = 0.$$

Thus, $m = f(n) = f(0) = 0$. This proves that $f(N) \cap \ker(f') = \{0\}$, meaning that $M = f(N) \oplus \ker(f')$ as desired. □

Ex 7. Let M be an R-module.

a) Show M is finitely generated if and only if it is a finite sum of cyclic R-modules.

b) Assume that M is the direct sum of a family $(M_i)_{i \in I}$ of nonzero submodules. Prove that I must be finite if M is finitely generated.

Proof.

a) $\implies$) Let M be finitely generated by the set $\{a_1, \ldots, a_n\}$. That is, there is no proper submodule of M that contains $\{a_1, \ldots, a_n\}$. We see that $\sum_{i=1}^n Ra_i$ is a finite sum of cyclic submodules. Since it is a submodule of M that contains $\{a_1, \ldots, a_n\}$, this proves that $M = \sum_{i=1}^n Ra_i$.

$\impliedby$) Let $M = \sum_{i=1}^n Ra_i$ for some $a_i \in M$. Thus, any element $m \in M$ can be written as $\sum_{i=1}^n r_i a_i$ for some $r_i \in R$. This means that if N is a submodule of M that contains the set $\{a_1, \ldots, a_n\}$, then N must contain m. Since $m \in M$ was arbitrary, we see that it must be that $M = N$ and thus that M is generated by the finite set $\{a_1, \ldots, a_n\}$.

b) If M is finitely generated, then by part (a), we know that M is a finite sum of cyclic R-modules, so $M = \sum_{j \leq n} Rx_j$ for some elements $x_j \in M$. Since we know that $M = \oplus_{i \in I} M_i$, we can represent each x_j as $x_j = \sum_{i \in I_j} m_i$ where I_j is some finite subset of I. Thus, if we let $I' = \cup_{j \leq n} I_j$, we get that $|I'| < \infty$ and $x_j \in \oplus_{i \in I'} M_i$ for every $j \leq n$. Since $\oplus_{i \in I'} M_i$ is a module containing the generating set, we get that $M = \oplus_{i \in I'} M_i$. Suppose there were an $i_0 \in I \backslash I'$. Then we could choose a nonzero $m \in M_{i_0} \subseteq M$ (we can do this because we assumed every M_i was nonzero). Since $M = \oplus_{i \in I'} M_i$, though, that'd mean $m = \sum_{i \in I'} m_i$, disproving that $\oplus_{i \in I} M_i$ uniquely represents every element of M. Thus, it must be that $I = I'$, and so I is finite. $\square$