Math 210A. Homework 1

1. Let R be an associative ring with identity. An element $u \in R$ is called a *unit* if it has a 2-sided multiplicative inverse: for some $u' \in R$, $uu' = u'u = 1$. The set of units is denoted $R^\times$. In general, computing $R^\times$ is very hard.

(i) The "2-sided" condition cannot be removed: find an infinite-dimensional vector space V over a field k and a k-linear map $f : V \to V$ admitting an inverse on one side but not the other. Deduce that the endomorphism ring $R = \mathrm{End}_k(V)$ contains elements having a 1-sided inverse but no 2-sided inverse.

(ii) Show that if R is a finite-dimensional algebra over a field k then the 2-sided condition can be dropped: if $r, r' \in R$ satisfy $rr' = 1$ then $r'r = 1$. (Hint: consider $x \mapsto r'x$ as a k-linear self-map of R.) Deduce that if such an R is nonzero and has no zero-divisors (i.e., nonzero $x, y \in R$ such that $xy = 0$) then $R^\times = R - \{0\}$.

(iii) Prove that $R^\times$ is group. Also prove that if $f : R \to R'$ is a ring homomorphism then $f(R^\times) \subseteq {R'}^\times$ and the restricted map $R^\times \to {R'}^\times$ is a group homomorphism.

2. Let $\{M_i\}_{i \in I}$ be a collection of left modules over an associative ring R. Give the direct product $P := \prod M_i$ componentwise left R-module structure, and define the *direct sum* $S := \oplus M_i \subseteq \prod M_i$ to be the *submodule* of tuples (m_i) for which all but finitely many m_i vanish (so $\oplus M_i = \prod M_i$ if all but finitely many M_i vanish, but not otherwise).

(i) Prove the following "universal mapping properties" of the direct product and direct sum in terms of the projections $\pi_i : P \to M_i$ and the inclusions $j_i : M_i \to S$. If $T_i : M \to M_i$ are R-linear maps *from* a left R-module M then there is a unique R-linear map $T : M \to P$ such that $\pi_i \circ T = T_i$ for all i, and if $L_i : M_i \to N$ are R-linear maps *to* a left R-module N then there is a unique R-linear map $L : S \to N$ such that $L \circ j_i = L_i$ for all i. In other words, there are unique ways to fill in commutative diagrams of linear maps

$$\begin{tikzcd} M \arrow[r, "?"] \arrow[dr, "T_i"'] & P \arrow[d, "\pi_i"] \\ & M_i \end{tikzcd} \qquad \begin{tikzcd} M_i \arrow[r, "j_i"] \arrow[dr, "L_i"'] & S \arrow[d, "?"] \\ & N \end{tikzcd}$$

when we let i vary through I. Note that the properties go in opposite directions: direct sums map to things, direct products receive maps from things.

(ii) For a left R-module M, explain why the specification of a linear isomorphism $\oplus_{i \in I} R \simeq M$ is equivalent to the specification of an indexed R-basis (i.e., linearly independent spanning set) $\{b_i\}_{i \in I}$ of M.

3. Let R be an associative ring. For $n \geq 1$, rigorously define the *polynomial ring* $R[X_1, \ldots, X_n]$ as follows. The set $R[X_1, \ldots, X_n]$ consists of functions $f : \mathbf{Z}_{\geq 0}^n \to R$ that vanish at all but finitely many elements of $\mathbf{Z}_{\geq 0}^n$; loosely speaking, f corresponds to $\sum f(J) X^J$ (as J varies through $\mathbf{Z}_{\geq 0}^n$).

(i) Define an R-module structure via pointwise operations on such f, and define the *product* $(f \cdot g)(J) = \sum_{J' + J'' = J} f(J') g(J'')$ (this is a finite sum). Show that $(f \cdot g)(J) = 0$ for all but finitely many J, and that this makes $R[X_1, \ldots, X_n]$ into an assocative ring containing R as a subring.

(ii) Define X_j to be the function $\mathbf{Z}_{\geq 0}^n \to R$ vanishing away from $(0, \ldots, 1, \ldots, 0)$ (1 in the jth slot), which it carries to 1. Prove that the X_j's are in the center of $R[X_1, \ldots, X_n]$ and that each $f \in R[X_1, \ldots, X_n]$ has a unique expression as a finite sum $\sum a_J X^J$ with $a_J \in R$ and $X^J := X_1^{j_1} \cdots X_n^{j_n}$ for $J = (j_1, \ldots, j_n)$.

(iii) Prove the following "universal mapping property": if $\phi : R \to A$ is a map of associative rings and $a_1, \ldots, a_n \in A$ commute with each other and with $\phi(R)$ then there is a unique ring map $R[X_1, \ldots, X_n] \to A$ extending ϕ and satisfying $X_i \mapsto a_i$ for all i. In case $R = \mathbf{Z}$, show that there is a unique ring map $\phi : \mathbf{Z} \to A$!

4. Let R be a commutative ring. The set $M_n(R)$ of $n \times n$ matrices with entries in R has an associative R-algebra structure given by the habitual formulas. Note that if $R' \to R$ is a map of commutative rings then applying it on matrix entries defines a map $M_n(R') \to M_n(R)$ of associative rings.

(i) Define the determinant $\det : M_n(R) \to R$ by the usual formula (as a sum indexed by the symmetric group S_n). Using the theory of determinants over a field, show that det is multiplicative when R is any domain. Then for any $m = (r_{ij})$ and $m' = (r'_{ij})$ in $M_n(R)$, use the unique ring map $\mathbf{Z}[x_{ij}, x'_{ij}] \to R$ satisfying $x_{ij} \mapsto r_{ij}$ and $x'_{ij} \mapsto r'_{ij}$ to deduce the multiplicativity of det in general (by reduction to the case of the ring $\mathbf{Z}[x_{ij}, x'_{ij}]$ that is a domain!).

(ii) Using the same technique, prove the Cayley-Hamilton theorem in $M_n(R)$ for any R (by reducing it to the case over an algebraically closed field, which you are assumed to have seen before).

(iii) Define the trace $\mathrm{Tr} : M_n(R) \to R$ by the usual formula $(r_{ij}) \mapsto \sum r_{ii}$. Prove that $\mathrm{Tr}(mm') = \mathrm{Tr}(m'm)$ by reducing it to the known case over a field.

(iv) Prove Cramer's Formula over any commutative ring (reducing to the known case over a field), so in particular $m \in M_n(R)^\times$ if and only if $\det(m) \in R^\times$.