2023 Fall Honors Algebra Exercise 5 (due on November 23 in recitation)

For submission of homework, please finish the 15 True/False problems, and choose 10 **problems from the standard ones and** 4 **problems from the more difficult ones. Mark the question numbers clearly.**

[A] = Artin, [DF] = Dummit and Foote, [DN] = Ding and Nie (Chinese), [H] = Hungerford.

5.1. **True/False questions.** (Only write T or F when submitting the solutions.)

(1) If $\varphi : M \to N$ is an injective R-module homomorphism, then $\ker(\varphi)$ is empty.
(2) Viewing R as a left module over itself, any left R-module homomorphism $\phi : R \to R$ satisfies $\phi(ab) = \phi(a)\phi(b)$ for $a, b \in R$.
(3) Let R be a ring and let M and N be left R-modules. Then $\mathrm{Hom}_R(M, N)$ is a left R-module.
(4) If M is a finitely generated R-module that is generated by n elements then every quotient of M may be generated by n (or fewer) elements.
(5) If M is a left R-module and if there exists $r \in R^\times$ such that $rm = 0$ for every $m \in M$, then $M = 0$.
(6) Let R be a ring. Any left R-module is also a $\mathbb{Z}$-module.
(7) Any ring R can be viewed as a left module over itself.
(8) Let M and N be two $\mathbb{Q}$-vector spaces and $\varphi : M \to N$ is a $\mathbb{Z}$-module homomorphism. Then φ is a $\mathbb{Q}$-linear map.
(9) $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) = 0$.
(10) Let K/F be an extension and $\alpha \in K$ is an algebraic element over F. Then $\alpha^2 + \alpha$ is algebraic over F.
(11) Every finite extension of fields is algebraic, and every algebraic extension of fields is finite.
(12) Let π be the usual ratio of a circle's circumference to its diameter. Then $\mathbb{Q}(\pi)$ is a normal extension of $\mathbb{Q}(\pi^2)$.
(13) If K/F is an algebraic extension, then for any intermediate field E, K is algebraic over E and E is algebraic over F.
(14) Let K/F be a finite field extension such that $[K : F] = p$ is a prime, then any element $\alpha \in K \backslash F$ generates K over F, i.e. $K = F(\alpha)$.
(15) Let K/F be a field extension and K_1 and K_2 intermediate fields. If K_1/F and K_2/F are algebraic, then K_1K_2/F is also algebraic.

5.2. **Warm-up questions.** (Do not submit solutions for the following questions)

Problem 5.2.1. [DF, page 343, problem 4]
Let $I_1, \dots, I_n$ be left ideals of R and let

$$M = \{(x_1, \dots, x_n) \mid x_i \in I_i, \text{ satisfiying } x_1 + x_2 + \cdots + x_n = 0\}.$$

Show that this M is a left R-submodule of $R^{\oplus n}$. Can you realize it as a kernel of some R-module homomorphism?

Problem 5.2.2. [DF, page 356, problem 12]
Let R be a commutative ring and let A, B and M be R-modules. Prove the following isomorphisms of R-modules:

(1) $\mathrm{Hom}_R(A \oplus B, M) \cong \mathrm{Hom}_R(A, M) \oplus \mathrm{Hom}_R(B, M)$,
(2) $\mathrm{Hom}_R(M, A \oplus B) \cong \mathrm{Hom}_R(M, A) \oplus \mathrm{Hom}_R(M, B)$.

Problem 5.2.3. Let $\varphi : A \to B$ be a homomorphisms of left R-modules, and let A' and B' be left R-submodules of A and B, respectively. Show that $\varphi(A')$ is a left R-submodule of B and $\varphi^{-1}(B')$ is a left R-submodule of A.

Problem 5.2.4. Let A, B, C, D be left R-modules, let $\varphi : A \to B$ and $\psi : C \to D$ be R-module homomorphisms. Show that there are natural homomorphisms of abelian groups:

$$\begin{array}{ccc} \mathrm{Hom}_R(B, C) & \longrightarrow & \mathrm{Hom}_R(A, C) \\ \eta & \longmapsto & \eta \circ \varphi \end{array} \qquad \begin{array}{ccc} \mathrm{Hom}_R(B, C) & \longrightarrow & \mathrm{Hom}_R(B, D) \\ \eta & \longmapsto & \psi \circ \eta. \end{array}$$

Problem 5.2.5. Let R be a commutative ring and let M be an R-module. Show that $\mathrm{Hom}_R(M, M)$ is an R-algebra, that is, there is a natural homomorphism $R \to \mathrm{Hom}_R(M, M)$ and its image lies in the center of the endomorphism ring $\mathrm{Hom}_R(M, M)$.

Problem 5.2.6. [DF, page 519, problem 2]
Show that $x^3 - 2x - 2$ is irreducible over $\mathbb{Q}$ and let θ be a root (namely $x + (x^3 - 2x - 2)$ in $\mathbb{Q}(\theta) = \mathbb{Q}[x]/(x^3 - 2x - 2)$. Compute $(1 + \theta)(1 + \theta + \theta^2)$ and $\frac{1+\theta}{1+\theta+\theta^2}$ in $\mathbb{Q}(\theta)$.

Problem 5.2.7. Prove that the cardinality of every finite field is a power of a prime.

Problem 5.2.8. Give an example of a field extension that is algebraic but not finite.

Problem 5.2.9. Give an example of a field extension K over F and two intermediate fields K_1 and K_2 of F such that

$$[K_1 K_2 : F] \neq [K_1 : F] \cdot [K_2 : F].$$

Problem 5.2.10. Give an example of a field F and two finite extensions K_1 and K_2 such that

- $[K_1 : F] \neq [K_2 : F]$
- K_1 is abstractly isomorphic to K_2.

5.3. **Standard questions.** (Please choose 10 problems from the following questions)

Problem 5.3.1. [DF, page 344, problem 8]
An element m of the R-module M is called a *torsion element* if $rm = 0$ for some nonzero element $r \in R$. The set of torsion elements is denoted $M_{\text{tor}} = \{m \in M \mid rm = 0 \text{ for some nonzero } r \in R\}$.

(1) Prove that if R is an integral domain then M_{tor} is a submodule of M (called the torsion submodule of M).
(2) Give an example of a ring R and an R-module M such that M_{tor} is not a submodule.

Problem 5.3.2. [DF, page 344, problem 9]
If M is a left R-module, the annihilator of M in R is defined to be

$$\text{Ann}_R(M) := \{r \in R \mid rm = 0 \text{ for all } m \in M\}.$$

Prove that $\text{Ann}_R(M)$ is a 2-sided ideal of R.

Problem 5.3.3. [DF, page 356, problem 7]
Let N be a submodule of M. Prove that if both M/N and N are finitely generated then so is M.

Problem 5.3.4. [DF, page 356, problems 9 and 10]
An R-module M is called *irreducible* if $M \neq 0$ and if 0 and M are the only submodules of M.

(1) Show that M is irreducible if and only if $M \neq 0$ and M is a cyclic module with any nonzero element as generator.
(2) Determine all the irreducible $\mathbb{Z}$-modules.
(3) Assume R is commutative. Show that an R-module M is irreducible if and only if M is isomorphic (as an R-module) to R/I where I is a maximal ideal of R.

Problem 5.3.5. Let R_1 and R_2 be rings and let $R := R_1 \times R_2$. Show that if M is an R-module, then we can canonically write $M \cong M_1 \oplus M_2$ with M_1 an R_1-module and M_2 an R_2-module.
Explicitly, let $e_1 = (1, 0)$ and $e_2 = (0, 1)$ in R. Then $M_i = e_i M$.

Problem 5.3.6. Consider $R = \mathbb{Z}[x]$, and the ideal $I = (2, x)$. As an R-module, I is generated by two elements $2, x$. What's the relation? If we write this as a surjective R-module homomorphism $R^{\oplus 2} \to I$ sending e_1 to 2 and e_2 to x, what is the kernel?

Problem 5.3.7. [A, page 487, problem 6.1]
Find a direct sum of cyclic groups which is isomorphic to the quotient

$$\mathbb{Z}^{\oplus 3}/A\mathbb{Z}^{\oplus 3} \qquad \text{with} \qquad A = \begin{pmatrix} 2 & 2 & 2 \\ 2 & 2 & 0 \\ 2 & 0 & 2 \end{pmatrix}.$$

Problem 5.3.8. [H, page 179, problems 9,10]
If $f : A \to A$ is a left R-module homomorphism such that $f \circ f = f$, then

$$A = \text{Ker}(f) \oplus \text{Im}(f).$$

More generally, Let $A, A_1, \ldots, A_n$ be left R-modules. Then $A \cong A_1 \oplus \cdots \oplus A_n$ if and only if for each $i = 1, \ldots, n$ there is a left R-module homomorphism $\varphi_i : A \to A$ such that $\text{Im}(\varphi_i) \cong A_i$; $\varphi_i \varphi_j = 0$ for $i \neq j$; and $\varphi_1 + \varphi_2 + \cdots + \varphi_n = 1_A$.

Problem 5.3.9. [H, page 180, problem 15]
If $f : A \to B$ and $g : B \to A$ are R-module homomorphisms such that $g \circ f = 1_A$, then $B = \operatorname{Im}(f) \oplus \operatorname{Ker}(g)$.

Problem 5.3.10. [DN, page 205, problem 1]
Let M be a finitely generated module over a PID R, and let $x_1, \ldots, x_n$ be a set of generators. Suppose that $y_1 = a_1x_1 + \cdots + a_nx_n$. If $(a_1, \ldots, a_n) = 1$, then there exist $y_2, \ldots, y_n \in M$ such that $y_1, \ldots, y_n$ generate of M.

Problem 5.3.11. [DN, page 205, problem 4]
Prove that over a PID R, a finitely generated torsion nonzero module M cannot be written as the direct sum of two nonzero submodules if and only if $M \simeq R/(p^e)$ for p a prime element of R and $e \geq 1$.

Problem 5.3.12. [DN, page 206, problem 12]
Let R be a commutative ring. If all submodules of a free module over R are free over R, then R is a PID.

Problem 5.3.13. [DF, page 311, problem 8]
Prove that $K_1 = \mathbb{F}_{11}[x]/(x^2 + 1)$ and $K_2 = \mathbb{F}_{11}[y]/(y^2 + 2y + 2)$ are both fields with 121 elements. Prove that the map which sends the element $p(\bar{x})$ of K_1 to the element $p(\bar{y} + 1)$ of K_2 (where p is any polynomial with coefficients in $\mathbb{F}_{11}$) is well defined and gives a ring (hence field) isomorphism from K_1 to K_2.

Problem 5.3.14. Let L be a field extension of K of degree n and V a vector space of dimension m over L. Show that, viewing V as a vector space over K, it has dimension mn, namely

$$\dim_K(V) = \dim_L(V) \cdot [L : K].$$

Problem 5.3.15. [DF, page 530, problems 7 and 8]
Prove that $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Conclude that $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$. Find the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$.
In general, let F be a field of characteristic $\neq 2$, and let D_1, D_2 be nonzero elements in F that are not squares. Prove that $F(\sqrt{D_1}, \sqrt{D_2})$ is of degree 4 over F if D_1D_2 is not a square in F and is of degree 2 over F if D_1D_2 is a square in F.
Remark: In the first case, we call $F(\sqrt{D_1}, \sqrt{D_2})$ a *biquadratic extension* of F.

Problem 5.3.16. [DF, page 530, problem 13]
Prove that if $[F(\alpha) : F]$ is odd, then $F(\alpha) = F(\alpha^2)$.

Problem 5.3.17. [DF, page 530, problem 16]
Let K/F be an algebraic extension and let R be a *ring* contained in K and containing F. Show that R is a subfield of K containing F.

Problem 5.3.18. [DF, page 530, problem 18]
Let k be a field and let $k(x)$ be the field of rational functions in x with coefficients from k. Let $t \in k(x)$ be the rational function $\frac{P(x)}{Q(x)}$ with relatively prime polynomials $P(x), Q(x) \in k[x]$, with $Q(x) \neq 0$. Then $k(x)$ is an extension of $k(t)$ and to compute its degree it is necessary to compute the minimal polynomial with coefficients in $k(t)$ satisfied by x.

(1) Show that the polynomial $P(X) - tQ(X)$ in the variable X and coefficients in $k(t)$ is irreducible over $k(t)$ and has x as a root. [By Gauss' Lemma this polynomial is

irreducible in $(k(t))[X]$ if and only if it is irreducible in $(k[t])[X]$. Then note that $(k[t])[X] = (k[X])[t]$.]

(2) Show that the degree of $P(X) - tQ(X)$ as a polynomial in X with coefficients in $k(t)$ is the maximum of the degrees of $P(x)$ and $Q(x)$.
(3) Show that $[k(x) : k(t)] = [k(x) : k(\frac{P(x)}{Q(x)})] = \max\{\deg P(x), \deg Q(x)\}$.

Problem 5.3.19. [H, page 241, problem 15]
In the field $\mathbb{C}(x)$, let $u = x^3/(x+1)$. Show that $\mathbb{C}(x)$ is a simple extension of the field $\mathbb{C}(u)$. What is $[\mathbb{C}(x) : \mathbb{C}(u)]$?

Problem 5.3.20. [DN, page 234, problem 9]
Prove that if K/F is an algebraic extension of fields, then any homomorphism $\sigma : K \to K$ that is identity on F is an isomorphism.

Problem 5.3.21. [DF, page 531, problems 19 and 21]
Let K be an extension of F of degree n.

(1) For any $a \in K$ prove that a acting by left multiplication on K is an F-linear transformation of K.
(2) Prove that K is isomorphic to a subfield of the ring of $n \times n$ matrices over F, so the ring of $n \times n$ matrices over F contains an isomorphic copy of every extension of F of degree $\leq n$.
(3) Make explicit this embedding for $K = \mathbb{Q}(\sqrt{D})$ and $F = \mathbb{Q}$ by choosing a basis of K by $\{1, \sqrt{D}\}$.

Problem 5.3.22. [DN, page 234, problem 8]
Let K/F be a field extension and K_1 and K_2 are intermediate fields. Show that
(1) If $[K_1 : F]$ and $[K_2 : F]$ are coprime, then $[K_1K_2 : F] = [K_1 : F] \cdot [K_2 : F]$.
(2) If K_1/F and K_2/F are algebraic, then so is K_1K_2/F.

Problem 5.3.23. [A, page 531, problem 3.7]
Decide whether or not i is in the field (a) $\mathbb{Q}(\sqrt{-2})$, (b) $\mathbb{Q}(\sqrt[4]{-2})$, (c) $\mathbb{Q}(\alpha)$, where $\alpha^3 + \alpha + 1 = 0$.

5.4. **More difficult questions.** (Please choose 4 problems from the following questions)

Problem 5.4.1 (Chinese Remainder Theorem for modules)**.** [DF, page 357, problems 16 and 17]

For any ideal I of R let IM be the submodule of M consisting of elements of the form $\sum_{i=1}^n a_i m_i$ with $a_i \in I$ and $m_i \in M$. (Caveat: the linear combination is needed here, namely, not all elements in IM can be written as am for $a \in I$ and $m \in M$.) Let $A_1, \dots, A_k$ be any left ideals in the ring R.

(1) Prove that the map
$$M \to M/A_1M \times \cdots \times M/A_kM \quad \text{defined by} \quad m \mapsto (m + A_1M, \dots, m + A_kM)$$
is an R-module homomorphism with kernel $A_1M \cap A_2M \cap \cdots \cap A_kM$.

(2) Assume further that R is commutative and the ideals $A_1, \dots, A_k$ are pairwise comaximal (i.e. $A_i + A_j = R$ for all $i \neq j$). Prove that
$$M/(A_1 \cdots A_k)M \cong M/A_1M \times \cdots \times M/A_kM.$$

Problem 5.4.2. [DF, page 357, problems 18 and 19]

Let R be a Principal Ideal Domain and let M be an R-module that is annihilated by the nonzero, proper ideal (a). Let $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be the unique factorization of a into distinct prime powers in R. Let M_i be the annihilator of $p_i^{\alpha_i}$ in M, i.e., M_i is the set $\{m \in M \mid p_i^{\alpha_i} m = 0\}$ — called the p_i-primary component of M.

(1) Prove that $M \cong M_1 \oplus M_2 \oplus \cdots \oplus M_k$.

(2) Show that if M is a finite abelian group of order $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ then, considered as a $\mathbb{Z}$-module, M is annihilated by (a), the p_i-primary component of M is the unique Sylow p_i-subgroup of M and M is isomorphic to the direct product of its Sylow subgroups.

Problem 5.4.3. [DF, page 356, problem 11]

Show that if M_1 and M_2 are irreducible R-modules (see the above problem for the definition of "irreducible modules"), then any nonzero R-module homomorphism from M_1 to M_2 is an isomorphism. Deduce that if M is irreducible then $\mathrm{End}_R(M)$ is a division ring. (This result is the module version of *Schur's Lemma*.)

Problem 5.4.4. [A. page 486, problem 5.7]

Let S be a subring of the ring $R = \mathbb{C}[t]$ which contains $\mathbb{C}$ and is not equal to $\mathbb{C}$. Prove that R is a finitely generated S-module. (Not difficult, just the way that it is phrased is a little confusing.)

Problem 5.4.5 (Jordan–Hölder theorem for modules)**.** Let R be a ring and let M be a left R-module. Suppose that we have two increasing sequences of submodules of M:
$$0 = A_0 \subseteq A_1 \subseteq \cdots \subseteq A_m = M, \quad \text{and} \quad 0 = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_n = M.$$
Prove that we can refine each sequence (by adding more submodules to the sequence) into
$$0 = A'_0 \subseteq A'_1 \subseteq \cdots \subseteq A'_\ell = M, \quad \text{and} \quad 0 = B'_0 \subseteq B'_1 \subseteq \cdots \subseteq B'_\ell = M$$
so that there is a permutation $\sigma \in S_\ell$ such that $A'_i/A'_{i-1} \cong B'_{\sigma(i)}/B'_{\sigma(i)-1}$ as left R-modules for each i.

Remark: The interesting case is when M has finite length: that is, there exists a sequence as above with each A_i/A_{i-1} irreducible R-module. This problem then says that the subquotients of any such increasing sequence of submodules are isomorphic, up to permutation. These subquotients are called the *Jordan–Hölder factors* of M.

Problem 5.4.6. [DN, page 206, problem 11]
Let R be a PID. Prove that every left ideal of $\mathrm{Mat}_{n\times n}(R)$ is principal.

Problem 5.4.7 (trace and norm)**.** Let L/K be a finite extension of degree n. Pick a basis of L as an n-dimensional K-vector space. Then for an element $x \in L$, multiplication by x is represented by a matrix $A_x \in \mathrm{M}_n(K)$.

(1) Show that the trace of A_x and the determinant of A_x are independent of the choice of basis of L as a K-vector space. They are denoted by $\mathrm{Tr}_{L/K}(x)$ and $N_{L/K}(x)$, respectively.

(2) Show that $\mathrm{Tr}_{L/K}$ is additive and $N_{L/K}$ is multiplicative.

(3) If E is an intermediate field of L/K and $\alpha \in E$, show that

$$\mathrm{Tr}_{L/K}(\alpha) = [L:E]\cdot \mathrm{Tr}_{E/K}(\alpha) \quad \text{and} \quad N_{L/K}(\alpha) = N_{L/K}(\alpha)^{[L:E]}.$$

(4) For $\alpha \in L$, let $m_{K,\alpha}(x) = x^h - a_1x^{h-1} + \cdots + (-1)^h a_h$ be the minimal polynomial. Then $\mathrm{Tr}_{L/K}(\alpha) = \frac{n}{h}\cdot a_1$ and $N_{L/K}(\alpha) = a_h^{n/h}$.

Problem 5.4.8 (Bimodules)**.** Let R and S be rings. An (R,S)-bimodule is an abelian group M that is equipped with a left R-module and a right S-module structure so that for $r \in R$, $s \in S$ and $m \in M$, we have

$$r(ms) = (rm)s.$$

(1) Show that if R is a commutative ring, then any left R-module M naturally admits a (R,R)-bimodule structure.
(2) Let M be an (R,S)-bimodule and N an R-module. Show that $\mathrm{Hom}_R(M,N)$ has a natural left S-module structure. (Somehow, we "canceled" the R-action.) On the other hand, $\mathrm{Hom}_R(N,M)$ admits a natural right S-module structure.

(Be careful about the left/right S-actions.)