Math 762 **Spring 2016**
Homework 3 **Drew Armstrong**

Problem 1. Yoneda's Lemma. We have seen that the bifunctor $\text{Hom}_{\mathcal{C}}(-,-) : \mathcal{C} \times \mathcal{C} \to \mathsf{Set}$ is analogous to a bilinear form on a K-vector space $\langle -,- \rangle : V \times V \to K$. Recall that a bilinear form $\langle -,- \rangle$ is called non-degenerate if for all vectors $x, y \in V$ we have

$$\langle x, z \rangle = \langle y, z \rangle \text{ for all } z \in V \quad \Longrightarrow \quad x = y.$$

The Yoneda Lemma tells us that the Hom bifunctor is "non-degenerate" in a similar way.

(a) For each object $X \in \mathcal{C}$ verify that $h^X := \text{Hom}_{\mathcal{C}}(X, -)$ defines a functor $\mathcal{C} \to \mathsf{Set}$.
(b) Given two objects $X, Y \in \mathcal{C}$ state what it means to have $h^X \approx h^Y$ as functors.
(c) Given two objects $X, Y \in \mathcal{C}$ and an isomorphism of functors $h^X \approx h^Y$, prove that we have an isomorphism of objects $X \approx Y$. [Hint: Let $\Phi : h^X \xrightarrow{\sim} h^Y$ be a natural isomorphism. Now consider the morphisms $\Phi_X(\text{id}_X) : Y \to X$ and $(\Phi_Y)^{-1}(\text{id}_Y) : X \to Y$.]

Problem 2. The Tower Law. Let R be a ring and let A, B be any sets. In this problem we will investigate the isomorphism of R-modules

$$(R^{\oplus A})^{\oplus B} \approx R^{\oplus (A \times B)}.$$

(a) For all sets $C \in \mathsf{Set}$ prove that there is a bijection

$$\text{Hom}_{\mathsf{Set}}(A \times B, C) \leftrightarrow \text{Hom}_{\mathsf{Set}}(B, \text{Hom}_{\mathsf{Set}}(A, C)).$$

(b) Given an R-module M we will define the R-module $M^{\oplus A}$ as a coproduct as in HW1.1(b). Prove that for all R-modules N there is a bijection

$$\text{Hom}_R(M^{\oplus A}, N) \leftrightarrow \text{Hom}_{\mathsf{Set}}(A, \text{Hom}_R(M, N)).$$

(c) Use parts (a) and (b) together with Yoneda's Lemma to prove the isomorphism of R-modules $(R^{\oplus A})^{\oplus B} \approx R^{\oplus (A \times B)}$. [Hint: You can assume without proof that the bijections from (a) and (b) are "natural" in their arguments.]
(d) Given a field extension $K \subseteq L$ prove that we can view L as a K-vector space. We will denote the dimension of this K-vector space by $[L : K]$. Now consider a chain of field extensions $K_1 \subseteq K_2 \subseteq K_3$. Use the isomorphism from part (c) to prove that

$$[K_3 : K_1] = [K_3 : K_2] \cdot [K_2 : K_1].$$

[Hint: Don't get your hands dirty.]

Problems 3–5 use the following definitions. Recall that a commutative R-algebra is a homomorphism $i : R \to S$ of commutative rings and an R-algebra morphism from $i_1 : R \to S_1$ to $i_2 : R \to S_2$ is a ring homomorphism $\varphi : S_1 \to S_2$ satisfying $\varphi \circ i_1 = i_2$. If $i : R \to S$ is an R-algebra, recall that for each element $a \in S$ there exists a unique R-algebra morphism $\varphi_a : R[x] \to S$ satisfying $\varphi_a(r) = i(r)$ for all $r \in R$ and $\varphi_a(x) = a$. [In other words, $R[x]$ is the free commutative R-algebra generated by one element.] We will say that

- $a \in S$ is transcendental over R if φ_a is injective,
- $a \in S$ is algebraic over R if φ_a is not injective,

and we will sometimes denote the image by $R[a] := \text{im}\, \varphi_a$. More generally, given an n-tuple of elements $A = \{a_1, a_2, \ldots, a_n\} \subseteq S$ there exists a unique R-algebra morphism $\varphi_A : R[x_1, \ldots, x_n] \to S$ such that $\varphi_A(r) = i(r)$ for all $r \in R$ and $\varphi_A(x_i) = a_i$ for all $a_i \in A$. [In other words, $R[x_1, \ldots, x_n]$ is the free commutative R-algebra generated by n elements.] We will say that

- $A \subseteq S$ is an R-algebraically independent set if φ_A is injective,

- $A \subseteq S$ is an R-algebraic generating set if φ_A is surjective.

We will denote the image by $R[A] := \operatorname{im} \varphi_A$ or $R[a_1, \ldots, a_n] := \operatorname{im} \varphi_A$, depending on context.

Problem 3. Algebraic Closure is Sometimes a Ring. Given an extension of commutative rings $R \subseteq S$ we will write $\operatorname{Alg}_R(S) \subseteq S$ for the set of elements of S that are algebraic over R. If $\operatorname{Alg}_R(S) = S$ we will say that S is algebraic over R. In this case we will also say that $R \subseteq S$ is an algebraic extension.

(a) Let $K \subseteq L$ be an extension of fields. If $[L : K] < \infty$, prove that L is algebraic over K.

(b) If $K \subseteq L$ is an extension of fields, prove that $\operatorname{Alg}_K(L)$ is a **subfield** of L. [Hint: Given $a, b \in \operatorname{Alg}_K(L)$, you want to show that $a - b$ and a/b are both in $\operatorname{Alg}_K(L)$. Let $K(a, b) \subseteq L$ be the intersection of all subfields of L that contain $K \cup \{a, b\}$. Use Problem 2(d) to show that $[K(a, b) : K] < \infty$. Then use part (a).]

(c) Now let $R \subseteq S$ be an extension of integral domains. Prove that $\operatorname{Alg}_R(S)$ is a **subring** of S. [Hint: Let $K \subseteq L$ be the corresponding fields of fractions. Prove that $\operatorname{Alg}_R(S) = S \cap \operatorname{Alg}_K(L)$ and then use part (b).]

Problem 4. Algebraic Over Algebraic is Sometimes Algebraic.

(a) Let $K \subseteq L$ be an extension of fields and consider an element $a \in \operatorname{Alg}_K(L)$. Prove that $K[a]$ is a field and that $[K[a] : K] < \infty$. [Hint: Since $K[x]$ is a PID, the kernel of the evaluation map $\varphi_a : K[x] \to S$ is generated by a single polynomial $m_a(x) \in K[x]$ called the minimal polynomial of a over K. Show that $m_a(x)$ is irreducible, hence $(m_a(x)) \subseteq K[x]$ is a maximal ideal, hence $K[a] \approx K[x]/(m_a(x))$ is a field. Then show that $[K[a] : K] = \deg m_a(x)$.]

(b) Let $K \subseteq L$ be an algebraic extension of fields such that L is finitely generated as a K-algebra. In this case prove that L is finite dimensional as a K-vector space. [Hint: Suppose that $L = K[a_1, \ldots, a_n]$ as a K-algebra and define $L_i := K[a_1, \ldots, a_i]$. Prove using part (a) and induction that L_{i+1} is a field and that $[L_{i+1} : L_i] < \infty$. Then use Problem 2(d).]

(c) Let R and S be integral domains. Prove that $R \subseteq S$ is an algebraic extension if and only if $\operatorname{Frac}(R) \subseteq \operatorname{Frac}(S)$ is an algebraic extension. [Hint: One direction uses Problem 3(b).]

(d) Now let $R_1 \subseteq R_2 \subseteq R_3$ be integral domains such $R_1 \subseteq R_2$ and $R_2 \subseteq R_3$ are algebraic extensions. In this case prove that $R_1 \subseteq R_3$ is also algebraic. [Hint: Let $K_1 \subseteq K_2 \subseteq K_3$ be the corresponding fields of fractions. By part (c) we know that $K_1 \subseteq K_2$ and $K_2 \subseteq K_3$ are algebraic. Now consider an arbitrary element $\alpha \in K_3$. We know that $\beta_0 + \beta_1\alpha + \cdots + \beta_n\alpha^n = 0$ for some elements $\beta_i \in K_2$, and hence α is algebraic over the subring $K_1[\beta_0, \ldots, \beta_n]$. Now use 4(b), 4(a), 2(d) and 3(a).]

Problem 5. Transcendence Degree Sometimes Exists. In this problem we will prove a version of "Steinitz Exchange" for algebras. Let $R \subseteq S$ be an extension of commutative rings. Given a subset $A \subseteq S$ of size n, let $\varphi_A : R[x_1, \ldots, x_n] \to S$ be the evaluation homomorphism with image $R[A] \subseteq S$. We will say that

- $A \subseteq S$ is R-algebraically independent if φ_A is injective,
- $A \subseteq S$ is R-almost generating if $R[A] \subseteq S$ is algebraic.

If $A \subseteq S$ is R-algebraically independent **and** R-almost generating we will call it a transcendence basis for the algebra $R \subseteq S$. Our goal is to prove that (for certain kinds of algebras) all transcendence bases have the same size.

(a) Let $R \subseteq S$ be an extension of **integral domains**. Let $A = \{a_1, \ldots, a_m\} \subseteq S$ be R-algebraically independent and let $B = \{b_1, \ldots, b_n\} \subseteq S$ be R-almost generating. Show that we can reorder the elements of B so that the set $\{a_1, b_2, \ldots, b_n\}$ is R-almost generating. [Hint: Since a_1 is algebraic over $R[b_1, \ldots, b_n]$ there exists a nontrivial polynomial relation $f(a_1, b_1, \ldots, b_n) = 0$. Since A is algebraically independent, at least one of the b_i must appear in this relation; without loss we can assume that b_1 appears. Now use Problem 3(c) and Problem 4(d).]

(b) If $m > n$, use induction on part (a) to obtain a contradiction.