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

Problem 1. Yoneda's Lemma. We have seen that the bifunctor $\mathrm{Hom}_{\mathcal{C}}(-,-) : \mathcal{C} \times \mathcal{C} \to \mathsf{Set}$ 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-degerenate 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 $h^X := \mathrm{Hom}_{\mathcal{C}}(X, -)$ 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 $\Phi_X(\mathrm{id}_X) : Y \to X$ and $(\Phi_Y)^{-1}(\mathrm{id}_Y) : X \to Y$.]

Proof. (a): To verify that $h^X := \mathrm{Hom}_{\mathcal{C}}(X, -)$ is a functor $\mathcal{C} \to \mathsf{Set}$ we must first say how it acts on morphisms in $\mathcal{C}$. There is only one obvious way to do this: given any morphism $\alpha : Y \to Z$ in $\mathcal{C}$ we will define the function

$$h^X(\alpha) : h^X(Y) \to h^X(Z)$$

by sending each morphism $\varphi : X \to Y$ to the morphism $\alpha \circ \varphi : X \to Y$. Note that for all objects $Y \in \mathcal{C}$ and morphisms $\varphi \in h^X(Y)$ we have $h^X(\mathrm{id}_Y)(\varphi) = \mathrm{id}_Y \circ \varphi = \varphi$ and hence

$$h^X(\mathrm{id}_Y) = \mathrm{id}_{h^X(Y)}.$$

Then note that for all morphisms $\alpha_1 : Y_1 \to Y_2$ and $\alpha_2 : Y_2 \to Y_3$ in $\mathcal{C}$ and $\varphi \in h^X(Y_1)$ we have $h^X(\alpha_2)\big(h^X(\alpha_1)(\varphi)\big) = \alpha_2 \circ (\alpha_1 \circ \varphi) = (\alpha_2 \circ \alpha_1) \circ \varphi = h^X(\alpha_2 \circ \alpha_1)$ and hence

$$h^X(\alpha_2 \circ \alpha_1) = h^X(\alpha_2) \circ h^X(\alpha_1).$$

(b): Given two objects $X, Y \in \mathcal{C}$ we say that $\Phi : h^X \to h^Y$ is a natural transformation if for each object $Z \in \mathcal{C}$ there is a morphism $\Phi_Z : h^X(Z) \to h^Y(Z)$ and for each morphism $\alpha : Z_1 \to Z_2$ there is a commutative diagram:

$$\begin{array}{ccc} h^X(Z_1) & \xrightarrow{\Phi_{Z_1}} & h^Y(Z_1) \\ {\scriptstyle h^X(\alpha)}\downarrow & & \downarrow{\scriptstyle h^Y(\alpha)} \\ h^X(Z_2) & \xrightarrow[\Phi_{Z_2}]{} & h^Y(Z_2) \end{array} \tag{1}$$

If each morphism Φ_Z is an isomorphism then we will say that $\Phi : h^X \to h^Y$ is a natural isomorphism and we will write $h^X \approx h^Y$.

(c): Now consider two objects $X, Y \in \mathcal{C}$ and assume that we have a natural isomorphism of functors $\Phi : h^X \xrightarrow{\sim} h^Y$. In this case we want to construct an isomorphism of objects $X \approx Y$. In particular, we need to find some morphisms $X \to Y$ and $Y \to X$.

The only morphisms in $\mathcal{C}$ that are guaranteed to exist are the identity morphisms (indeed, $\mathcal{C}$ might be a discrete category), so we start with these. We can apply $\Phi_X : h^X(X) \to h^Y(X)$ to the identity $\mathrm{id}_X \in h^X(X)$ to get a morphism $\varphi := \Phi_X(\mathrm{id}_X) \in h^Y(X)$ and since Φ_Y is invertible we can apply $(\Phi_Y)^{-1} : h^Y(Y) \to h^X(Y)$ to the identity $\mathrm{id}_Y \in h^Y(Y)$ to get a morphism $\psi := (\Phi_Y)^{-1}(\mathrm{id}_Y) \in h^X(Y)$. Now I claim that $\varphi \circ \psi = \mathrm{id}_X$ and $\psi \circ \varphi = \mathrm{id}_Y$, which will give us the desired isomorphism $X \approx Y$.

The only option we have now is to substitute the morphisms $\varphi : Y \to X$ and $\psi : X \to Y$ into the commutative square (1) and see what happens. First we substitute $\varphi : Y \to X$ to get

$$\begin{array}{ccc} h^X(Y) & \xrightarrow{\Phi_Y} & h^Y(Y) \\ {\scriptstyle h^X(\varphi)}\downarrow & & \downarrow{\scriptstyle h^Y(\varphi)} \\ h^X(X) & \xrightarrow[\Phi_X]{} & h^Y(X) \end{array}$$

and follow $\psi \in h^X(Y)$ from the top left corner to the bottom right corner to get

$$\begin{aligned} \Phi_X(h^X(\varphi)(\psi)) &= h^Y(\varphi)(\Phi_Y(\psi)) \\ \Phi_X(\varphi \circ \psi) &= \varphi \circ \Phi_Y(\psi) \\ \Phi_X(\varphi \circ \psi) &= \Phi_X(\mathrm{id}_X) \circ \Phi_Y((\Phi_Y)^{-1}(\mathrm{id}_Y)) \\ \Phi_X(\varphi \circ \psi) &= \Phi_X(\mathrm{id}_X) \circ \mathrm{id}_Y \\ \Phi_X(\varphi \circ \psi) &= \Phi_X(\mathrm{id}_X) \\ (\Phi_X)^{-1}(\Phi_X(\varphi \circ \psi)) &= (\Phi_X)^{-1}(\Phi_X(\mathrm{id}_X)) \\ \varphi \circ \psi &= \mathrm{id}_X. \end{aligned}$$

Then we substitute $\psi : X \to Y$ to get

$$\begin{array}{ccc} h^X(X) & \xrightarrow{\Phi_X} & h^Y(X) \\ {\scriptstyle h^X(\psi)}\downarrow & & \downarrow{\scriptstyle h^Y(\psi)} \\ h^X(Y) & \xrightarrow[\Phi_Y]{} & h^Y(Y) \end{array}$$

and follow $\varphi \in h^Y(X)$ from the top right corner to the bottom left corner to get

$$\begin{aligned} (\Phi_Y)^{-1}(h^Y(\psi)(\varphi)) &= h^X(\psi)((\Phi_X)^{-1}(\varphi)) \\ (\Phi_Y)^{-1}(\psi \circ \varphi) &= \psi \circ (\Phi_X)^{-1}(\varphi) \\ (\Phi_Y)^{-1}(\psi \circ \varphi) &= (\Phi_Y)^{-1}(\mathrm{id}_Y) \circ (\Phi_X)^{-1}(\Phi_X(\mathrm{id}_X)) \\ (\Phi_Y)^{-1}(\psi \circ \varphi) &= (\Phi_Y)^{-1}(\mathrm{id}_Y) \circ \mathrm{id}_X \\ (\Phi_Y)^{-1}(\psi \circ \varphi) &= (\Phi_Y)^{-1}(\mathrm{id}_Y) \\ \Phi_Y((\Phi_Y)^{-1}(\psi \circ \varphi)) &= \Phi_Y((\Phi_Y)^{-1}(\mathrm{id}_Y)) \\ \psi \circ \varphi &= \mathrm{id}_Y. \end{aligned}$$

□

[Remark: The notation in this proof is a nightmare. If you make the notation too simple you'll get confused; and if you make the notation too complicated you'll get confused. The philosophy behind Yoneda's Lemma is that we can replace the object $X \in \mathcal{C}$ by the functor $h^X : \mathcal{C} \to \mathrm{Set}$ without losing any information. Why would we want to do that? See Problem 2(c).]

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

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

(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

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

(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.]

Proof. (a): Previously we defined the Cartesian product $A \times B$ in terms of the existence of certain functions $C \to A \times B$, but now I'm asking you to consider functions $A \times B \to C$. That's kind of strange.

Given a function $f : A \times B \to C$ written as $(a, b) \mapsto f(a, b)$ we can define a function $\Phi_f : B \to \mathrm{Hom}_{\mathsf{Set}}(A, C)$ by $\Phi_f(b) := f(-, b)$. I claim that this defines a bijection

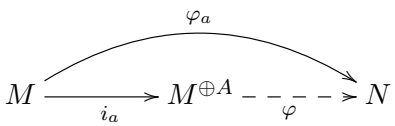
$$\Phi : \mathrm{Hom}_{\mathsf{Set}}(A \times B, C) \hookrightarrow\!\!\!\!\rightarrow \mathrm{Hom}_{\mathsf{Set}}(B, \mathrm{Hom}_{\mathsf{Set}}(A, C)).$$

Indeed, to see that Φ is **injective** suppose that we have $\Phi_f = \Phi_g$. Then for all $b \in B$ we must have $f(-, b) = \Phi_f(b) = \Phi_g(b) = g(-, b)$, which means that for all $a \in A$ we have $f(a, b) = g(a, b)$. Since this is true for all a and b we conclude that $f = g$. To see that Φ is **surjective**, consider any $F \in \mathrm{Hom}_{\mathsf{Set}}(B, \mathrm{Hom}_{\mathsf{Set}}(A, C))$. Then we note that $F = \Phi_f$ where $f : A \times B \to C$ is the function defined by $f(a, b) := F_b(a)$.

(b): Given an R-module M and a set A we will define the R-module $M^{\oplus A}$ as the coproduct of the indexed family $\{M_a\}_{a \in A}$, where $M = M_a$ for each $a \in A$. In other words, we assume that $M^{\oplus A}$ satisfies the following properties:

- There exists a morphism $i_a : M \to M^{\oplus A}$ for each $a \in A$.
- Given another R-module N and a family of morphisms $\varphi_a : M \to N$, there exists a unique morphism $\varphi : M^{\oplus A} \to N$ such that $\varphi \circ i_a = \varphi_a$ for each $a \in A$.

We can summarize this with the following diagram:



Now look carefully at this diagram. For each R-module homomorphism $\varphi : M^{\oplus A} \to N$ we certainly have a collection of morphisms $\{\varphi_a\}_{a \in A}$ defined by $\varphi_a := \varphi \circ i_a$. And, conversely, given any collection of morphisms $\varphi_a : M \to N$ we obtain a unique morphism $\varphi : M^{\oplus A} \to N$ satisfying $\varphi_a = i_a \circ \varphi$ for each $a \in A$. In other words, we have a bijection:

$$\begin{array}{ccc} \mathrm{Hom}_R(M^{\oplus A}, N) & \longleftrightarrow & \mathrm{Hom}_{\mathsf{Set}}(A, \mathrm{Hom}_R(M, N)) \\ \varphi & & \{\varphi_a\}_{a \in A} \end{array}$$

(c): Let N be any R-module. Assuming that the bijections from parts (a) and (b) are "natural", we obtain a chain of natural isomorphisms:

$$\begin{aligned}\mathrm{Hom}_R((R^{\oplus A})^{\oplus B}, N) &\cong \mathrm{Hom}_{\mathsf{Set}}(B, \mathrm{Hom}_R(R^{\oplus A}, N)) \\ &\cong \mathrm{Hom}_{\mathsf{Set}}(B, \mathrm{Hom}_{\mathsf{Set}}(A, \mathrm{Hom}_R(R, N))) \\ &\cong \mathrm{Hom}_{\mathsf{Set}}(A \times B, \mathrm{Hom}_R(R, N)) \\ &\cong \mathrm{Hom}_R(R^{\oplus(A\times B)}, N).\end{aligned}$$

In other words we have an isomorphism of functors $h^X \approx h^Y$ where $X = (R^{\oplus A})^{\oplus B}$ and $Y = R^{\oplus(A\times B)}$. It follows Yoneda's Lemma that we have an isomorphism of R-modules $X \approx Y$.

(d): Finally, let $K \subseteq L$ be an extension of fields. If we let $\iota : K \to L$ be the inclusion homomorphism then we can view L as a K-algebra. Then recall from HW2.5(b) that the definition $\lambda_a(b) := \iota(a)b = ab$ gives us a ring homomorphism $\lambda : K \to \mathrm{End}_{\mathsf{Ab}}(L)$. In other words, L is a K-vector space. We will denote its dimension by $[L : K]$.

Now consider a chain of field extensions $K_1 \subseteq K_2 \subseteq K_3$ so that K_2 is a K_1-vector space and K_3 is a K_2-vector space. Since all vector spaces are free there exist sets A and B such that $K_2 \approx K_1^{\oplus A}$ and $K_3 \approx K_2^{\oplus B}$. But then from part (c) we have

$$K_3 \approx K_2^{\oplus B} \approx ((K_1)^{\oplus A})^{\oplus B} \approx K_1^{\oplus(A\times B)}$$

and it follows that

$$\begin{aligned}[K_3 : K_1] &= [K_1^{\oplus(A\times B)} : K_1] \\ &= |A \times B| \\ &= |A| \cdot |B| \\ &= [K_2^{\oplus A} : K_2] \cdot [K_1^{\oplus B} : K_1] \\ &= [K_3 : K_2] \cdot [K_2 : K_1].\end{aligned}$$

□

[Remark: For all rings R and sets A, B we saw in class that there is an isomorphism of R-modules:

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

The slogan is that "dimension adds over direct sums". The proof of this isomorphism goes by the following yoga: since the "free" functor Set $\to R$-Mod defined by $A \mapsto R^{\oplus A}$ is left adjoint (to the "forgetful" functor R-Mod $\to$ Set), it commutes with coproducts. This result makes one wonder about the module $R^{\oplus(A\times B)}$. For dimension reasons we know that this module is not isomorphic to $R^{\oplus A} \oplus R^{\oplus B}$. In other words, the free functor does **not** commute with products, so it is not right adjoint to anything. But surely there is **something** interesting to say about the module $R^{\oplus(A\times B)}$. I thank Derek Elkins from StackExchange for telling me the interesting thing that became part (c).]

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 $R[a] := \operatorname{im} \varphi_a$. 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 $\operatorname{im} \varphi_A = R[A]$ or $\operatorname{im} \varphi_A = R[a_1, \ldots, a_n]$, 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).]

Proof. (a): Let $K \subseteq L$ be an extension of fields and assume that L is finite dimensional as a K-vector space. Now consider any element $a \in L$. If a were not algebraic over K then the set $\{1, a, a^2, \ldots\}$ would be an infinite K-linearly independent set. Contradiction.

(b): Consider a field extension $K \subseteq L$ and let $\operatorname{Alg}_K(L) \subseteq L$ denote the set of elements that are algebraic over K. We want to show that $\operatorname{Alg}_K(L)$ is a field. That is, given any two elements a and b in $\operatorname{Alg}_K(L)$ we want to show that $a - b$ and a/b are also in $\operatorname{Alg}_K(L)$. So consider the subfield $K(a, b) \subseteq L$, which is defined as the intersection of all subfields of L containing $K \cup \{a, b\}$. Similarly we can define the subfield $K(a) \subseteq K(a, b)$. Since a is algebraic over K we know from Problem 4(a) that $[K(a) : K] < \infty$ (the dimension is the degree of the minimal polynomial $m_a(x) \in K[x]$), and since b is algebraic over $K(a)$ (indeed, it's already algebraic over K) we know that $[K(a, b) : K(a)] = [K(a)(b) : K(a)] < \infty$. Then using the Tower Law from Problem 2(d) gives

$$[K(a, b) : K] = [K(a, b) : K(a)] \cdot [K(a) : K] < \infty$$

and it follows from part (a) that $K(a, b)$ is algebraic over K. Finally, since $a - b$ and a/b are both in $K(a, b)$ we conclude that they are both algebraic over K. [P.S.: Sorry that this proof used a result from Problem 4(a). I probably should have put all the field theory prerequisites into a separate problem, but that would have pushed the length of the homework assignment over two pages!]

(c): Now let $R \subseteq S$ be an extension of integral domains and let $K \subseteq L$ be the corresponding fields of fractions:

$$\begin{array}{ccccc} K & \longrightarrow & \operatorname{Alg}_K(L) & \longrightarrow & L \\ \uparrow & & \uparrow ? & & \uparrow \\ R & \longrightarrow & \operatorname{Alg}_R(S) & \longrightarrow & S \end{array}$$

To prove that $\operatorname{Alg}_R(S)$ is a subring of S we will show that $\operatorname{Alg}_R(S) = S \cap \operatorname{Alg}_K(L)$. Then since S and $\operatorname{Alg}_K(L)$ are both subrings of L (indeed we know from part (b) that $\operatorname{Alg}_K(L) \subseteq L$ is a sub**field**) it will follow that $\operatorname{Alg}_R(S)$ is a subring of L, hence also of S.

So consider any element $s \in \mathrm{Alg}_R(S)$. Since s is algebraic over R and since $R \subseteq K$ we conclude that s is algebraic over K, hence $s \in S \cap \mathrm{Alg}_K(L)$. Conversely, consider any element $s \in S \cap \mathrm{Alg}_K(L)$. Since s is algebraic over K there exist fractions $a_i/b_i \in K$ with $a_i \in R$ not all zero such that

$$\sum_i \frac{a_i}{b_i} s^i = 0. \tag{2}$$

Since R is a domain and since $b_i \neq 0$ for all i, the element $b := \prod_i b_i$ is nonzero. Multiplying both sides of (2) by b gives

$$\sum_i (a_i \hat{b}_i) s^i = 0,$$

where $\hat{b}_i = b/b_i \in R$. But we assumed that there exists j such that $a_j \neq 0$. Since $\hat{b}_j \neq 0$ and since R is a domain it follows that $a_j \hat{b}_j \neq 0$, and we conclude that $s \in \mathrm{Alg}_R(S)$ as desired. □

Problem 4. Algebraic Over Algebraic is Sometimes Algebraic.

(a) Let $K \subseteq L$ be an extension of fields and consider an element $a \in \mathrm{Alg}_K(L)$. 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 $\mathrm{Frac}(R) \subseteq \mathrm{Frac}(S)$ 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).]

Proof. (a): Let $K \subseteq L$ be a field extension and consider an element $a \in \mathrm{Alg}_K(L)$. Recall that we denote the image of the evaluation homomorphism $\varphi_a : K[x] \to L$ by $K[a]$. At first we only know that $K[a]$ is a subring of L, but I claim that it is in fact a sub**field**. To prove this, consider the kernel $\ker \varphi_a \subseteq K[x]$, which is nonzero by the assumption that a is algebraic. Since $K[x]$ is a PID [recall that Euclidean ⇒ PID] we must have $\ker \varphi_a = (m_a(x))$ for some polynomial $m_a(x) \in K[x]$, and since $a \in \mathrm{Alg}_K(L)$ we know that $m_a(x) \neq 0$. This polynomial is unique up to multiplication by units in $K[x]$ and the units of $K[x]$ are just the nonzero constants. Thus we can assume that $m_a(x)$ has leading coefficient 1 and we can call it "the" minimal polynomial of a over K (although this won't be necessary). Now assume for contradiction that $m_a(x)$ is **not irreducible**. That is, assume that we have $m_a(x) = f(x)g(x)$ where neither of $f(x)$ or $g(x)$ is a unit. Then substituting a (i.e., applying φ_a) gives

$$0 = m_a(a) = f(a)g(a)$$

and since K is a domain we conclude that $f(a) = 0$ or $g(a) = 0$. Without loss, suppose that $f(a) = 0$. This means that $f(x) \in \ker \varphi_a = (m_a(x))$ and hence $f(x) = m_a(x)q(x)$ for some $q(x) \in K[x]$. But then since $m_a(x) \neq 0$ and since $K[x]$ is a domain we have

$$\begin{aligned} m_a(x) &= f(x)g(x) \\ m_a(x) &= m_a(x)q(x)g(x) \\ m_a(x)(1 - q(x)g(x)) &= 0 \\ 1 - q(x)g(x) &= 0 \\ 1 &= q(x)g(x), \end{aligned}$$

which contradicts the fact that $g(x)$ is not a unit. Now since $m_a(x)$ is irreducible we know that the ideal $(m_a(x)) \subseteq K[x]$ is **maximal**. (Indeed, any (necessarily principal) ideal between $(m_a(x))$ and $K[x]$ would give rise to a proper divisor of $m_a(x)$.) Then from the Lattice Isomorphism Theorem we see that the ring $K[x]/(m_a(x))$ has no nontrivial ideals, hence its a field, hence it follows from the 1st Isomorphism Theorem that $K[a] = \operatorname{im} \varphi_a \approx K[a]/\ker \varphi_a = K[x]/(m_a(x))$ is also a field. If we denote by $K(a)$ the intersection of all subfields of L containing $K \cup \{a\}$ then since $K[a]$ contains $K \cup \{a\}$ we must have $K(a) \subseteq K[a]$. Conversely, since $K(a)$ contains $K \cup \{a\}$ it must contain all sums and products from this set, i.e., it must contain the whole ring $K[a]$. We conclude that $K[a] = K(a)$ (i.e. the smallest subring of L containing $K \cup \{a\}$ is also the smallest subfield containing $K \cup \{a\}$). Finally, suppose that $\deg m_a(x) = n$. In this case we will show that (the cosets generated by) $1, x, \ldots, x^{n-1}$ are a basis for the field $K[x]/(m_a(x))$ as a K-vector space. Indeed, let $f(x)+(m_a(x))$ be any nonzero element of $K[x]/(m_a(x))$. Then we can divide $f(x)$ by $m_a(x)$ to obtain $f(x) = q(x)m_a(x) + r(x)$ and since $f(x)$ is not in $(m_a(x))$ we must have $\deg r(x) < n$. But this implies that $f(x) + (m_a(x)) = r(x) + (m_a(x))$ is in the span of the cosets of $1, x, \ldots, x^{n-1}$. Furthermore this set is K-linearly independent since a nontrivial K-linear relation would imply that $g(x)+(m_a(x)) = 0+(m_a(x))$ for some polynomial $0 \neq g(x) \in K[x]$ with $\deg g(x) < n$. But this is impossible since $g(x) \in (m_a(x))$ implies that $m_a(x)$ divides $g(x)$ and hence $n = \deg m_a(x) \leq \deg g(x)$. We conclude that $1, x, \ldots, x^{n-1}$ is a basis for $K(a) \approx K[x]/(m_a(x))$ as a K-vector space and hence $[K(a) : K] = n$. [That does it I think. Part 4(a) summarizes a large chunk of MTH 562 for the benefit of students who didn't take MTH 562 (or didn't take it with me). Yes, maybe it would have been appropriate to put this in a separate problem along with parts 3(a) and 3(b).]

(b): Let $K \subseteq L$ be an algebraic field extension such that L is finitely generated as a K-algebra. This means that there exist elements $A = \{a_1, \ldots, a_n\} \subseteq L$ such that $L = K[A] = K[a_1, \ldots, a_n]$. We can interpret this as the image of the evaluation homomorphism $\varphi_A : K[x_1, \ldots, x_n] \to L$ or we can define it inductively by setting $L_i := K[a_1, \ldots, a_i]$ and $L_{i+1} := L_i[a_{i+1}]$ where $L_i[a_{i+1}]$ is the image of the evaluation homomorphism $\varphi_{a_{i+1}} : L_i \to L$. We will also set $L_0 := K$.

Now we will prove by induction that L_i is a field and that $[L_i : K] < \infty$. Indeed, we know that $L_0 = K$ is a field and that $[L_0 : K] = [K : K] = 1 < \infty$. Now assume for induction that L_i is a field and $[L_i : K] < \infty$. Then since $a_{i+1} \in \operatorname{Alg}_K(L) \subseteq \operatorname{Alg}_{L_i}(L)$ we have from part (a) that $L_{i+1} = L_i[a_{i+1}]$ is a field with $[L_{i+1} : L_i] < \infty$ and it follows from Problem 2(d) that

$$[L_{i+1} : K] = [L_{i+1} : L_i] \cdot [L_i : K] < \infty.$$

By induction we conclude that $[L : K] = [L_n : K] < \infty$ as desired.

(c): Now let $R \subseteq S$ be an extension of **integral domains**. In this case I claim that $R \subseteq S$ is algebraic if and only if $\operatorname{Frac}(R) \subseteq \operatorname{Frac}(S)$ is algebraic. To save notation let's define $K := \operatorname{Frac}(R)$ and $L := \operatorname{Frac}(S)$. Now recall from the proof of Problem 3(c) that

$$\operatorname{Alg}_R(S) = S \cap \operatorname{Alg}_K(L). \tag{3}$$

First suppose that L is algebraic over K so that $\mathrm{Alg}_K(L) = L$. Then equation (3) tells us that $\mathrm{Alg}_R(S) = S \cap L = S$, and hence S is algebraic over R. Conversely, suppose that S is algebraic over R so that $\mathrm{Alg}_R(S) = S$ and consider any fraction $s_1/s_2 \in L$. Since $S = \mathrm{Alg}_R(S) \subseteq \mathrm{Alg}_K(L)$ [this was the easy direction of equation (3)] we can think of s_1 and s_2 as elements of $\mathrm{Alg}_K(L)$. But we know from Problem 3(b) that $\mathrm{Alg}_K(L)$ is a field, which implies that $s_1/s_2 \in \mathrm{Alg}_K(L)$ and hence $\mathrm{Alg}_K(L) = L$ as desired.

(d): Finally let $R_1 \subseteq R_2 \subseteq R_3$ be integral domains such that $R_1 \subseteq R_2$ and $R_2 \subseteq R_3$ are algebraic extensions. In this case we will prove that $R_1 \subseteq R_3$ is algebraic. [In the original version of the HW I told you to assume that $R_1 \subseteq R_2$ and $R_2 \subseteq R_3$ are finitely generated as algebras. Thanks to David Udumyan for showing me that this is not necessary.]

First let $K_1 \subseteq K_2 \subseteq K_3$ be the corresponding fields of fractions. From part (c) we know that $K_1 \subseteq K_2$ and $K_2 \subseteq K_3$ are algebraic field extensions. If we can show that $K_1 \subseteq K_3$ is algebraic then it will again follow from part (c) that $R_1 \subseteq R_3$ is algebraic. So consider any element $a \in K_3$. Since $K_3 = \mathrm{Alg}_{K_2}(K_3)$ we can write

$$0 = b_0 + b_1 a + \cdots + b_n a^n \tag{4}$$

for some elements $b_0, b_1, \ldots, b_n \in K_2$. But then since $K_2 = \mathrm{Alg}_{K_1}(K_2)$ we have from the proof of part (b) that $K_1[b_1, \ldots, b_n]$ is a field and that $[K_1[b_1, \ldots, b_n] : K_1] < \infty$. Similarly, since a is algebraic over $K_1[b_1, \ldots, b_n]$ by equation (4), we have that $K_1[b_1, \ldots, b_n][a]$ is a field and that $[K_1[b_1, \ldots, b_n][a] : K_1[b_1, \ldots, b_n]] < \infty$. Now the Tower Law [Problem 2(d)] tells us that

$$[K_1[b_1, \ldots, b_n][a] : K_1] = [K_1[b_1, \ldots, b_n][a] : K_1[b_1, \ldots, b_n]] \cdot [K_1[b_1, \ldots, b_n] : K_1] < \infty$$

and then part (a) implies that $K[b_1, \ldots, b_n][a]$ is algebraic over K_1. In particular, $a \in K_3$ is algebraic over K_1. Since a was an arbitrary element of K_3 this proves the result. □

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.

Proof. Let $R \subseteq S$ be an extension of integral domains. Let $A = \{a_1, \ldots, a_m\} \subseteq S$ be an R-algebraically independent set and let $B = \{b_1, \ldots, b_n\} \subseteq S$ be an R-almost generating set. We wish to prove that $m \leq n$. Since parts (a) and (b) are essentially the same thing, I'll do them at the same time. [I was trying to be pedagogical in the way I wrote them problem. Maybe it was unnecessary.]

Assume for contradiction that $m > n$. In this case we will prove that $\{a_1, \ldots, a_n\}$ is an R-almost generating set. Then the fact that $a_{n+1} \in S$ is algebraic over the subring $R[a_1, \ldots, a_n]$ provides the desired contradiction.

So fix some $0 \leq k < n$ and assume for induction that the set

$$\{a_1, \ldots, a_k, b_{k+1}, \ldots, b_n\}$$

is R-almost generating. (Certainly this true when $k = 0$.) By definition of "almost generating" this implies that there exists a nonzero polynomial $f(x_0, \ldots, x_n) \in R[x_0, \ldots, x_n]$ such that

$$f(a_1, \ldots, a_k, a_{k+1}, b_{k+1}, \ldots, b_n) = 0. \tag{5}$$

At least one of the variables $x_{k+1}, \ldots, x_n$ must occur in the polynomial f since otherwise we obtain a nontrivial polynomial relation $f(a_1, \ldots, a_{k+1}) = 0$, contradicting the fact that A is R-algebraically independent. Without loss of generality, assume that the variable x_{k+1} occurs. Then the relation (5) then tells us that the element $b_{k+1} \in S$ is algebraic over the subring $R[a_1, \ldots, a_{k+1}, b_{k+2}, \ldots, b_n]$ and Problem 3(c) tells us that the whole ring

$$R[a_1, \ldots, a_{k+1}, b_{k+1}, \ldots, b_n] = R[a_1, \ldots, a_{k+1}, b_{k+2}, \ldots, b_n][b_{k+1}]$$

is algebraic over $R[a_1, \ldots, a_{k+1}, b_{k+2}, \ldots, b_n]$. Since S is algebraic over $R[a_1, \ldots, a_{k+1}, b_{k+1}, \ldots, b_n]$ (indeed, the a_{k+1} is not even necessary) we conclude from Problem 4(d) that S is algebraic over $R[a_1, \ldots, a_{k+1}, b_{k+2}, \ldots, b_n]$ and hence

$$\{a_1, \ldots, a_{k+1}, b_{k+2}, \ldots, b_n\}$$

is an R-almost generating set for S. By induction it now follows that $\{a_1, \ldots, a_n\}$ is an R-almost generating set for S, which gives the desired contradiction.

Epilogue: Let $R \subseteq S$ be an extension of integral domains and let $A, B \subseteq S$ be two R-transcendence bases. Applying our result in one direction gives $|A| \leq |B|$ and applying it in the other direction gives $|B| \leq |A|$. We conclude that all R-transcendence bases have the same cardinality. [The proof probably extends to transcendence bases of transfinite cardinality, but I don't care. To learn more about the general concept of "Steinitz exchange" see the paper of Saunders Mac Lane: "A lattice formulation for transcendence degrees and p-bases" (1938).] $\square$

[Remark: In summary, we have the following important structure theorem for algebras. Let $R \subseteq S$ be an extension of integral domains. We can express this as a series of three extensions

$$R \subseteq R[A] \subseteq R[A]^{\oplus B} \subseteq S,$$

where A is a transcendence basis for S as an R-algebra and B is a basis for S as an $R[A]$-module. The results of HW2 and HW3 tell us that the cardinalities of A and B are well-defined. Furthermore, we know that the quotient $S/R[A]^{\oplus B}$ is a torsion $R[A]$-module. If this torsion module is in fact the zero module (i.e., if $R[A]^{\oplus B} = S$) then we might use the words "Cohen-Macaulay" to describe the algebra $R \subseteq S$.

It's possible to remove the hypothesis that S is an integral domain (it's not possible to remove this hypothesis on R) but to do so we have to replace the notion of "algebraic extension" by the notion of "integral extension". The general result in this direction is the "Noether Normalization Lemma"; it is approximately twice as difficult as the results we proved on HW2 and HW3.]

[Meta-Remark: Why do we care? Well, if we want to use algebras and modules as a foundation for mathematics then we need to know this kind of stuff. But **why** do we want to use algebras and modules as a foundation for mathematics? Well, do you have a better idea?]