Math 121. Homework 1

1. This exercise constructs the "field of fractions" of a domain R. Consider ordered pairs (a, b) with $a, b \in R$ and $b \neq 0$. Declare (a, b) and (c, d) to be *equivalent* (denoted $(a, b) \sim (c, d)$) if $ad = bc$.

(i) Show that $\sim$ is an an equivalence relation (i.e., $(a, b) \sim (a, b)$, $(a, b) \sim (c, d)$ if and only if $(c, d) \sim (a, b)$, and $\sim$ is transitive).

(ii) Check that if $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$ then $(ad + bc, bd) \sim (a'd' + b'c', b'd')$ and $(ac, bd) \sim (a'c', b'd')$ (note that $bd, b'd' \neq 0$ since R is a domain).

(iii) Let F denote the set of equivalence classes for $\sim$, and let a/b denote the equivalence class of (a, b). Using (ii), show that the binary operations

$$(a/b) + (c/d) := (ad + bc)/(bd), \quad (a/b)(c/d) := ac/bd$$

on F are *well-defined* and make F into a ring with identity elements $0/1$ and $1/1$ for addition and multiplication respectively. For the ring axioms, just write out the verification that addition is associative by using the cancellation law in domains (and check the rest in private). Show that $r \mapsto r/1$ is an injective ring homomorphism $i : R \to F$.

(iv) Show that $a/b = 0/1$ if and only if $a = 0$, and that if $a, b \neq 0$ then b/a is a multiplicative inverse of a/b; deduce that F is a field. We call it the *field of fractions of* R. (§7.5 in the course text gives a lengthy development of this in a more general setting; it is better to think about this on your own without looking at the text.) For $R = k[X]$ with a field k, F is denoted $k(X)$.

In algebra, the construction of ring homomorphisms is very important. The remaining exercises provide rigorous means by which we construct such maps in various contexts. These are mostly "intuitively obvious", so the only point is to carefully write out the details once.

2. Let R be a domain with fraction field F, and $i : R \to F$ the natural inclusion map of rings.

(i) Prove that F is the "smallest" field into which R injects in the sense that for any *injective* ring homomorphism $f : R \to k$ into a field k, there is a unique map of fields $j : F \to k$ extending f (i.e., $j \circ i = f$). Hint: use injectivity of f to show that for $a, b \in R$ with $b \neq 0$, there is only one possibility for $j(a/b)$, and then show that the unique possibility really "works".

(ii) The conclusion in (i) fails if $\ker f \neq 0$: for $a \in k$, prove the evaluation-at-a map $f : k[X] \to k$ does not extend to a ring homomorphism $k(X) \to k$. (Where would $1/(X - a)$ go?)

3. Let R be a ring. Let S be an R-algebra. Prove that for any $s \in S$, there is a unique R-algebra map $F : R[X] \to S$ such that $F : X \mapsto s$. In down-to-earth terms, this says that to map $R[X]$ to S as an *R-algebra* is the "same" as choosing an element of S (the place where X goes).

Using a fixed identification $\mathbf{C} = \mathbf{R}[X]/(X^2 + 1)$ (i.e., fixing a choice i of $\sqrt{-1}$ in $\mathbf{C}$), what data do we need on an $\mathbf{R}$-algebra A in order to get a map of $\mathbf{R}$-algebras $\mathbf{C} \to A$?

4. (i) Generalize the construction in class to rigorously define the R-algebra $R[X_1, \dots, X_n]$ for any $n \geq 1$ and verify associativity for multiplication (check the rest in private). Prove a mapping property for R-algebras analogous to Exercise 3 above (using evaluation at an ordered n-tuple in S). Do *not* use the recursive method of definition $R[X_1, \dots, X_n] := (R[X_1, \dots, X_{n-1}])[X_n]$ as in the course text; treat $X_1, \dots, X_n$ on an equal footing in the definition.

(ii) (Extra Credit) If I is *any* non-empty set (perhaps infinite, maybe even uncountable), give a definition (and mapping property) for an R-algebra $R[X_i]_{i \in I}$ with indeterminates indexed by the set I. Intuitively, elements of $R[X_i]_{i \in I}$ are *finite* R-linear combinations of monomials in the X_i's.

Hint: you may find it helpful to think about functions $I \to \mathbf{N}$ vanishing away from a finite set; e.g., $X_{i_1}^{e_1} \cdots X_{i_n}^{e_n}$ should correspond to the function $I \to \mathbf{N}$ that carries i_j to e_j and vanishes away from the finite subset $\{i_1, \dots, i_n\}$ of I.