Math 121. Homework 2

1. Let R be a ring and I an ideal. Consider the natural ring map $\pi : R \to R/I$ given by $\pi(x) = x \bmod I$. Prove that a ring map $\varphi : R \to S$ can be factored as $\varphi = \psi \circ \pi$ for some $\psi : R/I \to S$ if and only if $I \subseteq \ker(\varphi)$, in which case ψ is unique. This gives a "universal" way to construct maps from the quotient ring R/I.

2. Show that $\mathbf{Z}$ is the most basic ring in the sense that for any ring R, there is a unique map of *rings* $f_R : \mathbf{Z} \to R$. That is, every ring is a $\mathbf{Z}$-algebra in a unique way. (Informally, $f_R(n)$ consists of adding 1_R to itself n times if $n > 0$.) For the proof, you may take for granted the Principle of Recursive Definition, which asserts that for any set X, equipped with a choice of $x \in X$ and a map of sets $\varphi : X \to X$ (the 'recursive formula'), there is a unique map of sets $\psi : \mathbf{N} \to X$ satisfying $\psi(1) = x$ and $\psi(n+1) = \varphi(\psi(n))$ for all $n \in \mathbf{N}$.

In particular, if $g : R \to S$ is any map of rings, then $g \circ f_R = f_S$.

3. (*i*) For a ring R, the kernel of the natural map f_R from Exercise 2 is an ideal in $\mathbf{Z}$, so it has the form $c(R)\mathbf{Z}$ for a unique $c(R) \geq 0$. We call $c(R)$ the *characteristic* of R. Intuitively, this is the least number of times we have to add 1_R to itself until we get 0_R (provided $c(R) > 0$). Show that the characteristic of a domain is either 0 or prime and that if $g : R \to S$ is a map of rings, then necessarily the characteristic of R is a $\mathbf{Z}$-multiple of the characteristic of S.

(*ii*) If $g : R \to S$ is injective (e.g., $S = R[X]$ or S is the fraction field of a domain R with g the natural map), show that $c(R) = c(S)$. Give an example (with g not injective) where $c(R) \neq c(S)$. Do there exist ring homomorphisms between fields with different characteristics? How about between domains with different characteristics?

(*iii*) If R is a ring with prime characteristic p, show that $(x+y)^{p^n} = x^{p^n} + y^{p^n}$ for all $x, y \in R$ and $n \geq 0$.

4. (*i*) Prove that for $m > 0$, the ring $\mathbf{Z}/m\mathbf{Z}$ is a field if and only if m is a prime. Note that $\mathbf{Z}/m\mathbf{Z}$ has characteristic m. For a prime $p > 0$, we often write $\mathbf{F}_p$ instead of $\mathbf{Z}/p\mathbf{Z}$ when we wish to view it as a field (rather that just as a group).

(*ii*) Let k be a field. If k has characteristic 0, show there is a unique map of fields $\mathbf{Q} \to k$. If k has characteristic p, show there is a unique map of fields $\mathbf{F}_p \to k$. Thus, $\mathbf{Q}$ and $\mathbf{F}_p$ are the most basic fields.

5. (i) Let k be a field and A a k-algebra with *finite dimension* as a k-vector space (e.g., $A = k[X]/(f)$ for nonzero $f \in k[X]$). If A is a domain, use linear algebra over k with the multiplication map $M_a : x \mapsto ax$ for nonzero $a \in A$ to prove that A is a field.

(ii) Prove that any domain whose underlying set is finite is necessarily a field.

6. If L/k is an extension field and $a \in L$, then $k[a]$ denotes the k-subalgebra of L generated by a; i.e., the image of the unique k-algebra map $k[X] \to L$ sending X to a (equivalently, the set of elements of L of the form $g(a)$ with $g \in k[X]$).

(i) Let L/k be a degree 2 extension of fields. If k has characteristic different from 2, show that $L = k[a]$ with $a^2 \in k$, $a \notin k$. Be sure to prove a "quadratic formula" in a suitable setting if you choose to use it.

(ii) If k has characteristic 2 and $X^2 + X + 1$ is irreducible in $k[X]$ (e.g., $k = \mathbf{F}_2$), then prove that $k[X]/(X^2 + X + 1)$ is a degree 2 extension field of k and *cannot* be expressed in the form $k[a]$ with $a^2 \in k$ (since the PID $k[X]$ is a UFD, under these hypotheses $k[X]/(X^2 + X + 1)$ is a domain and therefore a field).