Math 594. Homework 6 (due March 5)

1. Let R be a ring. Prove that for all $x \in R$, $0_R \cdot x = 0_R$ and $(-1_R)x = -x$.

In algebra, the construction of maps between rings is very important. The next five exercises provide the rigorous means by which we will be able to construct 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 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 on the quotient ring R/I.

3. Let R be a ring. Let S be an R-algebra. Prove that for any $s \in S$, there exists a unique R-algebra map $f : R[X] \to S$ such that $f(X) = s$. In down-to-earth terms, mapping $R[X]$ to S (as an R-*algebra*) is the 'same' as choosing an element of S.

Using a fixed identification $\mathbf{C} = \mathbf{R}[X]/(X^2 + 1)$ (i.e., fixing a choice 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. Generalize the sequence-based construction in class to rigorously define the R-algebra $R[X_1, \dots, X_n]$ for any $n \geq 1$ and prove a mapping property for R-algebras analogous to Exercise 3 above. If I is *any* set, give a definition (and mapping property) for an R-algebra $R[X_i]$, with indeterminates indexed by the set I (or we could even take the indeterminates to *be* the elements of I; the distinction is just psychological and notational). For this latter construction, you may find it helpful to use the set of functions from I to $\mathbf{N}$ which vanish on all but finitely many elements.

5. Let R be a domain with fraction field F, and let $i : R \to F$ be the usual inclusion map of rings. Prove that F is the 'smallest' field to which R injects in the sense that for any injective ring map $f : R \to k$ from R to a field k, there is a unique map of fields $j : F \to k$ so that $f = j \circ i$. Is this true if we don't require f to be injective?

$*$ 6. 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. To prove this, 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 $n \in \mathbf{N}$ (if you have time, think about how to rigorously prove this Principle from the Peano axioms).

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

7. (*i*) For a ring R, the kernel of the natural map f_R from Exercise 6 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 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 R with R a domain, 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 maps 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 $n \geq 0$.

$*$ 8. (*i*) Prove that for $m > 0$, the ring $\mathbf{Z}/m$ is a field if and only if m is a prime. Note that $\mathbf{Z}/m$ has characteristic m. For a prime $p > 0$, we often write $\mathbf{F}_p$ instead of $\mathbf{Z}/p$ 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, then there is a unique map of fields $\mathbf{Q} \to k$. If k has characteristic p, then there is a unique map of fields $\mathbf{F}_p \to k$. Thus, $\mathbf{Q}$ and $\mathbf{F}_p$ are the most 'basic' fields.

$*$ 9. (*i*) Let $f : R \to S$ be a map of rings. Show that this induces a natural group map between unit groups $f^\times : R^\times \to S^\times$. If $r \in R$ satisfies $r^n = 0$ for some $n \geq 1$, then for any $u \in R$, show that $u \in R^\times$ if and only if $u + r \in R^\times$ (hint: recall the geometric series for $(1+x)^{-1}$). Consider the case $S = R/I$, with f the natural map. Prove $f^\times$ is surjective with $f^{-1}(S^\times) = R^\times$ if every $x \in I$ satisfies $x^{n_x} = 0$ for some $n_x \geq 1$ (the converse is not generally true).

(*ii*) For a prime p, determine the unit group $((\mathbf{Z}/p^2)[X])^\times$. Also determine $(\mathbf{Z}[X]/(X^{1000}))^\times$.

10. Let k be a field and A a k-algebra with finite dimension as a k-vector space. If A is a domain, prove that A is a field. Also, prove that if A is a domain whose underlying set is finite, then A is a field. Why does this imply that $1/(2^{1/3} + 4^{1/5})$ can be expressed as a $\mathbf{Q}$-linear polynomial in $\alpha = 2^{1/3}$ and $\beta = 4^{1/5}$?

11. 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.

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 $a^2 \in k$ (for this, you may take for granted the unique factorization theorem in $k[X]$, which we will prove later, in order to know that under the above hypotheses, $k[X]/(X^2 + X + 1)$ is a domain and therefore a field).