Math 594. Solutions to Homework 6

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

Since $0_R + 0_R = 0_R$, if we multiply both sides by x and add $-(0_R \cdot x)$ to both sides and use the associative law for addition, we get $0_R \cdot x = 0_R$. Since $1_R + -1_R = 0_R$, multiplying through by x and using the first part, together with $1_R \cdot x = x$, we find that $(-1_R)x$ is the additive inverse to x.

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.

Viewing R/I first as the quotient of additive groups, we see the existence and uniqueness of ψ as an additive group map, by the mapping properties of quotients from group theory. The only issue is to check that ψ is a ring map. This follows readily from the construction of ψ and the fact that $R \to R/I$ is a map of rings (since I is an ideal).

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 $\mathbf{C} \to A$?

Let $\varphi : R \to S$ be the structure map. Then if f exists, we must have

$$f\left(\sum a_i X^i\right) = \sum f(a_i) f(X)^i = \sum \varphi(a_i) s^i,$$

since f is a map of R-algebras. Because of the unique representation of every element of $R[X]$ as a polynomial expression in X with coefficients in R, we can use the above formula to *define* f as a map of sets (i.e., it is well-defined). Now one checks from the definition of the ring structure on $R[X]$ that f is a map of R-algebras.

By Exercise 2, together with the above, an $\mathbf{R}$-algebra map $\mathbf{C} \to A$ is equivalent to choosing $a \in A$ with $a^2 = -1$ (though in a general A, there could well be infinitely many such a).

4. Generalize the sequence-based construction in class to rigorously define the R-algebra $R[X_1, \ldots, X_n]$ 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.

Let H be the set of functions $M : I \to \mathbf{N}$ with the property that $M(i) = 0$ for all but finitely many $i \in I$ (M stands for 'monomial'). Let 0_H denote the zero function and let M_i denote the function which sends i to 1 and everything else to 0. Define $R[X_i]$ to be the set of functions $f : H \to R$ with $f(M) = 0_R$ for almost all $M \in H$ and define X_i to be the function given by $X(M_i) = 1_R$ and $X(M) = 0_R$ for $M \neq M_i$. We define $\mathbf{0}$ and $\mathbf{1}$ in $R[X_i]$ by $\mathbf{0}(M) = 0_R$ for all $M \in H$ and $\mathbf{1}(M) = 0_R$ for $M \neq 0_H$ and $\mathbf{1}(0_H) = 1$. Addition is defined by $(f+g)(M) = f(M) + g(M)$ (which does vanish for all but finitely many M), and we verify immediately that with $(-f)(M) = -(f(M))$, $(R[X_i], +, \mathbf{0})$ is an additive group.

In order to define multiplication, we use the formula

$$(fg)(M) = \sum_{N_1 + N_2 = M} f(N_1) g(N_2),$$

where N_1 and N_2 run through all (finitely many) elements of H whose pointwise sum is M. Clearly this does vanish for all but finitely many M, and so defines an element in $R[X_i]$. It is now a tedious exercise to check that this makes $R[X_i]$ a ring, with $\mathbf{1}$ an identity for multiplication.

We then verify that the map of sets $j : R \to R[X_i]$ given by $j(r)(0_H) = r$, $j(r)(M) = 0_R$ for $M \neq 0_H$ is an injective map of rings, so $R[X_i]$ is an R-algebra. We now always write r instead of $j(r)$ to simplify notation. One checks by the definitions that $f \in R[X_i]$ can be uniquely written as a polynomial in X_i's with coefficients in R, namely

$$f = \sum_{f(M) \neq 0_R} \left(f(M) \prod_{M(i) \neq 0} X_i^{M(i)} \right),$$

with the usual convention that a sum over the empty set is $\mathbf{0}$ and a product over the empty set is $\mathbf{1}$.

Given any R-algebra $\varphi : R \to S$ and $s_i \in S$ for all $i \in I$, it follows from the definition of the ring structure above that the set-theoretic map $e : R[X_i] \to S$ given by

$$e(f) = \sum_{f(M) \neq 0_R} \left(\varphi(f(M)) \prod_{M(i) \neq 0} s_i^{M(i)} \right)$$

is an R-algebra map. It is then readily checked to be the unique one which sends X_i to s_i.

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?

All maps between fields are necessarily injective, so the answer to the last part is 'no'. It is easy to see that $i : r \mapsto r/1$ is injective (here, r/s denotes the residue class of (r, s) in F). From the definitions it is clear that $r/s = (r/1)(s/1)^{-1}$, so if j exists, then

$$j(r/s) = j(i(r))j(i(s))^{-1}) = j(i(r))j(i(s))^{-1} = f(r)f(s)^{-1},$$

so j is unique. As for existence, use this formula to *define* j, noting that $f(s)^{-1}$ makes sense for non-zero $s \in R$, as f is injective and k is a field. One then checks this is well-defined (i.e., independent of choice of numerator and denominator representatives) and gives a ring map with the desired properties.

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 $g \circ f_R = f_S$.

Once the first part is proven, the second follows from the fact that $g \circ f_R$ satisfies the property that uniquely determine f_S. As for existence and uniqueness of f_R in general, an induction argument shows that if f and f' are two such maps, then since $f(1) = f'(1) = 1_R$, then $f(n) = f'(n)$ for all $n > 0$. Since f and f' are additive group maps, we see $f(n) = f'(n)$ for $n \leq 0$ also, so uniqueness follows.

As for existence, define $f(n)$ for $n > 0$ using $f(1) = 1_R$ and $f(n+1) = f(n) + 1_R$ (i.e., Principle of Recursive Definition with $X = R$ and $\psi(x) = x + 1_R$). Then define $f(0) = 0_R$ and $f(n) = -f(-n)$ for $n < 0$. By the uniqueness part of the Principle of Recursive Definition, we have $-f(-n) = f(n)$ for all $n \in \mathbf{Z}$. In order to prove $f(m+n) = f(m) + f(n)$ for all $m, n \in \mathbf{Z}$, we therefore need only consider the case with $m > 0$. We can therefore induct on m, and the case $m = 1$ follows from the definitions. To prove $f(mn) = f(m)f(n)$, we again may assume that $m > 0$ (recall Exercise 1 too) and again can induct on m, the case $m = 1$ being clear.

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. 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 $n \geq 0$.

(*i*) Since $g \circ f_R = f_S$, $\ker(f_R) \subseteq \ker(f_S)$. Thus, $c(S)|c(R)$. Since $\mathbf{Z}/c(R)$ injects into R, if R is a domain, then so is $\mathbf{Z}/c(R)$. This clear prevents $c(R)$ from being composite. Note that 1 is the characteristic of only the zero ring, which we ruled out from being a domain in our definitions!

(*ii*) Since g is injective, $f_S = g \circ f_R$ and f_R have the same kernel. The map $\mathbf{Z} \to \mathbf{Z}/2$ is a map between domains with different characteristics, but maps of fields are always injective and so there are no maps between fields with different characteristics.

(*iii*) We induct on n, the case $n = 1$ following from the binomial formula (proof valid in any ring, or else check in $\mathbf{Z}[X, Y]$ and use Exercises 4 and 6) and the fact that for $0 < i < p$, $p!/i!(p-i)!$ is divisible by p.

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.

(*i*) By Exercise 10, $\mathbf{Z}/m$ is a domain if and only if it is a field. Since it has characteristic m, it can only be a domain for prime m (Exercise 7). It is immediate from the definitions and unique factorization in $\mathbf{Z}$ that $\mathbf{Z}/p$ *is* a domain for a prime p.

(*ii*) By Exercise 6, there is a unique map of ring $\mathbf{Z} \to k$. By Exercise 5, we are done if this map is injective — that is, if k has characteristic 0. Otherwise, by Exercise 2 we are done if k has characteristic p.

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 $(\mathbf{Z}[X]/(X^{1000}))^\times$.

(*i*) If $r \in R^\times$, so $rr' = 1_R$, then $f(r)f(r') = f(rr') = f(1_R) = 1_S$, so $f(r) \in S^\times$. So it is clear how to define $f^\times$. Now say $r \in R$ is nilpotent (i.e., some $r^n = 0$). Since $-r$ is also nilpotent (by Exercise 1), we need only check that for $u \in R^\times$, we have $u + r \in R^\times$. Scaling through by u^{-1}, we are reduced to the case $u = 1$. Now use the hint to consider a truncated Taylor series.

For I as given, if $f(r)$ is a unit, then $rr' = 1 + x$ with x nilpotent, so rr' is a unit. Thus, r is a unit. Since f is surjective, we are done.

(*ii*) Using (*i*) with I the ideal generated by p, we see that $(\mathbf{Z}/p^2)[X]^\times$ is the set of polynomials of the form $a_0 + pf$ with $a_0 \in \mathbf{Z}/p^2$ not a multiple of p. Taking I to be the ideal generated by X in the second case, the units in $\mathbf{Z}[X]/X^{1000}$ are elements with a constant term of 1 or -1.

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 $\beta = 4^{1/5}$?

For non-zero $a \in A$, the map $x \mapsto ax$ is an injective k-linear map from A to itself. Since $\dim_k(A)$ is finite, this map must be surjective and therefore hits 1, so a is a unit. In the second case, use cardinality arguments to replace linear algebra. Taking $A = \mathbf{Q}[\alpha, \beta]$ and noting that $\dim_{\mathbf{Q}} A$ is finite (since $\alpha^3 = 2$ and $\beta^5 = 4$) shows that A is a field, so the visibly nonzero $\alpha + \beta \in A$ has a multiplicative inverse in A (which is an expression of the desired type).

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 $a^2 \in k$.

By linear algebra, we can find a basis of the form $\{1, a\}$. Expressing a^2 as a linear combination of 1 and a, we can complete the square if $\mathrm{char}(k) \neq 2$. This gives a 'better'a with $a^2 \in k$.

Note that under the hypothesis in the second part, the quotient ring is actually a domain (and thus a field). For example, $k = \mathbf{F}_2$ is such a k. Any possible a must have a unique representative of the form $A + BX$ with $B \neq 0$, $A, B \in k$. Since k has characteristic 2, we see that a^2 is represented by $A^2 + B^2 + B^2X$, which is never in k for $B \neq 0$.