Math 614, Fall 2008

Problem Set #2: Solutions

1. In the category of sets, the empty set is an initial object and a set with one element is a final object. In the category of commutative rings with identity,$\mathbb{Z}$ is an initial object (the unique map $\mathbb{Z} \to R$ sends n to $n \cdot 1_R$) and the 0 ring is a final object. In the category of modules over a ring R, the 0 module is both an initial and a final object.

2. $f = h$ because, by the universal mapping property of localization, the map $R \to T$ given by $gf = hf$ factors uniquely through S (since $f(W)$ consists of units of S, $gf(W)$ consists of units of T). $\square$

Alternatively, every element of S has the form r/w where $r \in R$ and $w \in W$. Then $(gf)(w)g(r/w) = g(w/1)g(r/w) = g(r/1) = (gf)(r) = (hf)(r) = h(r/1) = h(w/1)h(r/w) = (hf)(w)h(r/w)$. Since $(gf)(w) = (hf)(w)$, we can conclude that $g(r/w) = h(r/w)$ provided that $(gf)(w)$ is invertible in T. But $(gf)(w) = g(w/1)$ has inverse $g(1/w)$, as required. $\square$

3. We have the localization homomorphism $R \to U^{-1}R$ that sends $r \mapsto r/1$. Since the image of W consists of units in $U^{-1}R$, there is a unique R-algebra homomorphism $W^{-1}R \to U^{-1}R$ that sends r/w to r/w (the two symbols have different meanings: in the second instance, w is to be thought of as an element of U). Since the image of $\widetilde{V}$ consists of units in $U^{-1}R$ we have a unique homomorphism $\alpha : \widetilde{V}^{-1}S \cong U^{-1}R$ that sends $(r/w)/(v/1) \mapsto r/(vw)$. Similarly, since the image of $U = VW$ consists of units in $\widetilde{V}^{-1}S$ (the inverse of vw is $(1/w)/v$), we have a unique R-algebra homomorphism $\beta : U^{-1}R \to \widetilde{V}^{-1}S$ that sends $r/(vw) \mapsto (r/w)/(v/1)$. It is now obvious that $\alpha \circ \beta$ is the identity on $U^{-1}R$ and that $\beta \circ \alpha$ is the identity on $\widetilde{V}^{-1}S$. $\square$

4. Let $s = \dfrac{1+\sqrt{p}}{2}$. This element is integral over $\mathbb{Z}$, since it is a root of $x^2 - x - k = 0$. Clearly, s is in the fraction field of $\mathbb{Z}[\sqrt{p}]$, which is $\mathbb{Q}[\sqrt{p}]$. Note that $\sqrt{p} = 2s - 1$, so $\mathbb{Z}[\sqrt{p}] \subseteq \mathbb{Z}[s]$. Since $s^2 = s + k$, the set $\mathbb{Z} + \mathbb{Z}s$ is already closed under multiplication, and so $\mathbb{Z}[s] = \mathbb{Z} + \mathbb{Z}s$. Now suppose that $a + b\sqrt{p}$ is integral over $\mathbb{Z}$, where $a, b \in \mathbb{Q}$. We shall show that $a + b\sqrt{p} \in \mathbb{Z}$. If $b = 0$, this follows because $\mathbb{Z}$ is a PID, hence, a UFD, and is normal. If $b \neq 0$ the minimal monic polynomial of $a + b\sqrt{p}$ over $\mathbb{Q}$ is $(x - a)^2 - b^2p = 0$. Since $\mathbb{Z}$ is normal, if $a + b\sqrt{5}$ is integral over $\mathbb{Z}$, we must have that the coefficients are in $\mathbb{Z}$, i.e., that $-2a$ and $a^2 - b^2p$ are in $\mathbb{Z}$. Thus, we we may assume that $a = n/2$, where $n \in \mathbb{Z}$. By subtracting ns we obtain a new integral element of the form $c\sqrt{p}$, where c is rational. To complete the proof, it suffices to show c must be an integer. Then $(c\sqrt{p})^2$ is integral over $\mathbb{Z}$ and rational, and so must be an integer. Since pc^2 is an integer, we can write $c^2 = n/p$. But when we write $c = r/s$ is in lowest terms, $r, s \in \mathbb{Z}$, $s > 0$, r^2/s^2 is also in lowest terms, which implies that s^2 divides p. Thus, $s = 1$, as required. $\square$

5. (a) Let $A = R - Q$ and $B = R - Q'$. Then a prime is contained in both P and Q if and only if it is disjoint from both A and B, and this holds if and only if it is disjoint from AB, since the complement of a prime is a multiplicative system. Thus, there exists a prime contained in both Q and Q' if and only if AB does not contain the element 0, i.e., if and only if there do not exist $a \in R - Q$ and $b \in R - Q'$ such that $ab = 0$. If there is no such prime, then with $a \in A$ and $b \in B$ such that $ab = 0$, we have that

$Q \in D(a) = \mathrm{Spec}\,(R) - V(a)$ and $Q' \in D(b)$ while $D(a) \cap D(b) = \emptyset$: the fact that $ab = 0$ shows that $V(a) \cup V(b) = \mathrm{Spec}\,(R)$. $\square$

(b) Let Q and Q' be distinct prime ideals. Then there is no prime ideal contained in both, since there cannot be a strict containment of two primes. By part (a), Q and Q' have disjoint open neighborhoods. This proves that X is a Hausdorff space. It was shown in class that $\mathrm{Spec}\,(R)$ is always quasicompact, so that X is compact. A quasicompact subspace must then be closed. Let two points be given. Then the first has an open neighborhood of the form $D(a)$ that does not contain the second, and $D(a)$ is quasicompact and so closed as well as open.

6. Let M be the set of monomials $x_1^{k_1} \cdots x_n^{k_n}$ in the x_i such that $0 \leq k_i < n_i$ for every i. We claim that the image of M spans the quotient $T = S/(F_1, \ldots, F_n)S$ as an R-module. If not, there is some monomial μ whose image is not in the R-span T_0 of M. Choose such a μ of smallest possible degree. Some x_i must occur with exponent at least n_i in μ, or else μ would be in T_0. Hence, we can write $\mu = x_i^{n_i}\nu$ for some monomial ν. The equation $F_i = 0$ holds in T and may be used to espress $x_i^{n_i}$ as an R-linear combination of lower degree monomials. Multiply by ν. This enables one to write $\mu = x_i^{n_i}\nu$ as an R-linear combination of lower degree monomials, and these are in T_0. Hence, $\mu \in T_0$, a contradiction. $\square$