QUESTION (HD0308): Let $S = \{X^{\alpha} : \alpha \in Q^{+}\}$ where Q^{+} denotes the set of nonnegative rational numbers. Let R be the semi-group ring $Q[S]$ and if P is a nonzero prime ideal of R, must $P^{-1} = R$?

ANSWER: The answer is **not generally**! To understand the answer you need to know that (i) R is a directed union of PID's $R_n = Q[X^{\frac{1}{n}}]$, where n ranges over integers ≥ 1, (ii) R is a Bezout domain and (iii) in a Bezout domain every irreducible element is a prime. If you do not know some or all of these requirements then go read the requirements before reading further.

If you know all these then consider the element $X-2$ in R. I claim that $X-2$ is irreducible in R and hence a prime. If $X-2 = fg$ with f,g nonunits in R then because R is a directed union of R_n 's, $X-2 = fg$ with f,g nonunits in R_n for some natural number n. But for each $n > 1$, $X-2 = (X^{\frac{1}{n}})^n - 2$ which is irreducible in $Q[X^{\frac{1}{n}}]$ using Eisenstein's irreducibility criterion. So $X-2$ is not reducible in the Bezout domain R and hence is a prime. Thus $P = (X-2)R$ is a prime ideal in R, but $P^{-1} = \frac{1}{X-2}R \supsetneq R$.

Requirements:

(i) R can be regarded as a directed union (or direct limit) of the polynomial rings $R_n = Q[X^{\frac{1}{n}}]$. By directed union we mean that $R = \bigcup_{n\geq 1} R_n$ such that if there are some natural numbers $n_1, n_2 \ldots n_r$ then there is a natural number m (divisible by each of n_i) such that $\bigcup_{i=1}^{i=r} R_{n_i} \subseteq R_m$.

(ii). Using the fact that $R = \bigcup_{n\geq 1} R_n$ is a directed union, and the fact that each of R_n is a PID we can show that R is a Bezout domain (every finitely generated ideal is principal). This can be established as follows: Let $f,g \in R$ then there is a natural number n such that $f,g \in R_n$ for some natural number n. Since R_n is a PID there exists $h \in R_n$ such that $fR_n + gR_n = hR_n$. But since R_n is a subring of R we have $R_nR = R$ and so $(fR_n + gR_n)R = hR_nR$, which gives $fR + gR = hR$. Thus every two generated ideal in R is principal and this can be used to show that every finitely generated ideal of R is principal.

(iii). Using $fR + gR = hR$, for every pair of nonzero elements $f,g \in R$ we can say that for each pair of nonzero elements $f,g \in R$ there exist elements $h,u,v \in R$ such that $uf + vg = h$ such that $h \mid f$ and $h \mid g$ in R. The element h has the property that each d that divides both f and g also divides h. But this is the characteristic property of the GCD (greatest common divisor) of two integers, in elementary number theory. For this reason the h in $fR + gR = hR$ is called a GCD of f and g. Using the elementary number theory language we can say that if c is a GCD of a and b in R then there exist $r,s \in R$ such that $c = ra + sb$. (We know that for some $k \in R$ we have $aR + bR = kR$. Since c is a GCD of a,b and k is a common factor of a,b we conclude that $k \mid c$ and since c divides both a and b we conclude that $c \mid k$. Thus c and k are associates and so $cR = kR$ and we conclude that $aR + bR = cR$, but then there exist $r,s \in R$ such that $c = ra + sb$. Again, using the number theory language we can say that two elements of R are coprime if they do not have a nonunit common divisor. But then in R, as in the case of integers, if a and b are coprime then there exist $r, s \in R$ such that $ra + sb = 1$. Now let f be an irreducible element in R. To show that f is a prime we have to establish that $f \mid ab$ implies $f \mid a$ or $f \mid b$. For this we suppose that f does not divide a then because f is irreducible f and a are coprime. But then there must be r and s such that $rf + sa = 1$. Multiplying both sides of the equation by b we get $rfb + sab = b$. Recalling that $f \mid ab$ we decide that f divides the left hand side of $rfb + sab = b$ and so $f \mid b$. But then $f \mid ab$ implies $f \mid a$ or $f \mid b$ and so f is a prime.

NOTES: (a). The description of requirement (iii) is stated for R but it works generally for all Bezout domains and essentially it is a review of the basic number theory or the basic ring theory.

(b). I mentioned Eisenstein's irreducibility criterion. If you do not remember it here it is (stated for the ring of integers Z): If $f = \sum a_i X^i \in Z[X]$, deg($f$) ≥ 1 and p is an irreducible element of Z such that $p \nmid a_n : p \mid a_i$ for $i = 0, 1, \ldots n-1; p^2 \nmid a_0$ then f is irreducible in $Q[X]$. (For a more general statement look up Theorem 6.15 (page 164) of [Thomas Hungerford, Algebra, Springer-Verlag, 1974].)