Subrings of the rational numbers

The proof of the following basic result is fairly elementary, but it is not always easy to find a proof in undergraduate algebra texts.

THEOREM. *Suppose that A is a subdomain of the rational numbers. Then there is a set of primes $\mathbf{S}$ such that A is isomorphic to the ring $\mathbf{Z}_{\mathbf{S}}$ generated by the integers and the inverses of all elements of $\mathbf{Z}$.*

The ring $\mathbf{Z}_{\mathbf{S}}$ consists of all fractions of the form a/b where a is an integer and b is a monomial in the elements of $\mathbf{S}$ (by convention, the monomial with zero factors is equal to 1, so the integers are contained in $\mathbf{Z}_{\mathbf{S}}$). It is straightforward to check that $\mathbf{Z}_{\mathbf{S}}$ is closed under addition and multiplication and hence is a subdomain of the rationals.

Proof. Since A is a subdomain it must contain both 0 and 1. Also, if n is a positive integer which lies in A, then it follows that $n+1$ also lies in A and hence A by induction A contains all positive integers. Since A is also closed under taking negatives, it also follows that all negative integers lie in A and therefore all of $\mathbf{Z}$ is contained in A.

Now let $A^\times$ is the group of units in A, and let $\mathbf{S}$ be the intersection of $A^\times$ with the set of positive primes. It follows immediately that A contains $\mathbf{Z}_{\mathbf{S}}$, so we only need to show the reverse inclusion.

We might as well assume that A strictly contains the integers, and hence it contains some rational number r/s where $r, s \in \mathbf{Z}$ and $s \neq 0$; of course we may choose r and s so that they have no common factors other than ± 1. Suppose now that we are given a rational number $k/n \in A$, where k and n are integers such that $n > 2$ and the greatest common divisor of k and n equals 1. By the Chinese Remainder Theorem we can find integers x and y such that $xk = yn + 1$ and therefore we have

$$\frac{1}{n} \quad = \quad \frac{xk - yn}{n} \quad = \quad x \cdot \frac{k}{n} \; - \; y \quad \in \quad A \; .$$

Suppose now that p is a prime divisor of n,and write $n = pq$. It then follows that

$$\frac{1}{p} \quad = \quad \frac{q}{n} \quad = \quad q \cdot \frac{1}{n} \quad \in \quad A$$

and hence $1/p \in \mathbf{S}$. In fact, this is true for **every** prime dividing n, and therefore we have $1/n \in \mathbf{Z}_{\mathbf{S}}$. The latter in turn implies that $k/n \in \mathbf{Z}_{\mathbf{S}}$, and therefore we see that the rational number k/n belongs to $\mathbf{Z}_{\mathbf{S}}$ as required.∎

GENERALIZATION TO PRINCIPAL IDEAL DOMAINS. The proof of the theorem can be modified to yield a similar result if $\mathbf{Z}$ and $\mathbf{Q}$ are replaced by a prinicpal ideal domain D and its quotient field F.∎