THE SUBRINGS OF THE RING OF RATIONAL NUMBERS

GEORGE MCNULTY

The project of the MATH 701I students was to discover as many subrings of the ring of rational numbers as possible. Here I give one way to tackle this problem.

What might make this task hard? For one thing, it is open-ended. How do you know when you are done? Is there a reasonable way to describe each of the subrings? How many subrings are there anyway?

There are two obvious subrings: The ring of integers and the whole ring of rational numbers. Since 0 and 1 must belong to each subring and each subring must be closed under $+, \cdot$, and $-$, it is pretty clear that every integer is in each of the subrings. So the ring of integers is a subring of every subring of the rationals. So with respect to the ordering by the subring relation, the ring of integers is the smallest subring. Likewise, the ring of all rationals is the largest. We are after the subrings in between.

Now one of the things that makes the ring of rationals different from the ring of integers is that every nonzero rational has a multiplicative inverse that belongs to the ring of rationals, whereas in the ring of integers the only elements that have multiplicative inverses belonging to the ring of integers are 1 and -1. We could expect that a subring $\mathbf{R}$ of the ring of rationals might have more invertible elements than are available in the integers but still not have all its nonzero elements invertible.

Perhaps it is possible to get a better understanding of the subring $\mathbf{R}$ by considering its invertible elements. To begin with the simplest case, suppose $b \in R$ and $\frac{1}{b} \in R$ where b is a positive integer. Just by using the fact that R is closed under multiplication we see that $\frac{1}{b^2} \in R$ and indeed that $\frac{1}{b^n} \in R$ for each natural number n. What else must be in R? Suppose d is an integer that divides b. Pick an integer q so that $b = dq$. Then $\frac{1}{d} = q\frac{1}{dq} = q\frac{1}{b} \in R$, since every integer ($q$ in this case) belongs to R and R is closed under multiplication. So $\frac{1}{d} \in R$ for every factor d of b. In particular, this means that $\frac{1}{p} \in R$ for every prime factor p and b. We can reason in the reverse direction as well: if $\frac{1}{p} \in R$ for all the prime factors of b, then $\frac{1}{b} \in R$, since we can obtain it by way of multiplication from the $\frac{1}{p}$'s.

This suggests that we consider the set $\left\{p \mid \frac{1}{p} \in R \text{ and } p \text{ is a prime number}\right\}$. Let us call this set $\mathsf{P}(\mathbf{R})$. It is the set of primes whose multiplicative inverses lie in the subring $\mathbf{R}$. We could even think of P has a function from the set of all subrings of the ring of rationals into the collection of all subsets of the set of prime numbers.

If we could show that the function P was a one-to-one correspondence this would amount to a pretty good description of what the subrings were.

Claim
If $\mathbf{R}$ and $\mathbf{S}$ are subrings of the ring of rational numbers and $\mathsf{P}(\mathbf{R}) = \mathsf{P}(\mathbf{S})$, then $\mathbf{R} = \mathbf{S}$.

This claim asserts that P is one-to-one. To prove it we have to demonstrate that R and S have the same elements. It helps to realize that every rational number has the form $\frac{a}{b}$ where a and b are integers, b is positive, and a and b are relatively prime. This representation of a rational in "lowest terms" is unique. Since a and b are relatively prime, pick integers u and v so that

$$au + bv = 1.$$

Dividing both sides by b we obtain

$$u\frac{a}{b} + v = \frac{1}{b}$$

Since all the integers belong to R and this set is closed under addition and multiplication, we see that

$$\frac{a}{b} \in R \text{ if and only if } \frac{1}{b} \in R.$$

But our reasoning above shows

$$\frac{1}{b} \in R \text{ if and only if } \frac{1}{p} \in R \text{ for all prime factors } p \text{ of } b$$

Putting these two things together we get

$$\frac{a}{b} \in R \text{ if and only if } \frac{1}{p} \in R \text{ for all prime factors } p \text{ of } b.$$

By the same reasoning

$$\frac{a}{b} \in S \text{ if and only if } \frac{1}{p} \in S \text{ for all prime factors } p \text{ of } b.$$

Since $\mathsf{P}(\mathbf{R}) = \mathsf{P}(\mathbf{S})$ we conclude that

$$\frac{a}{b} \in R \text{ if and only if } \frac{a}{b} \in S.$$

So $R = S$ and P is one-to-one, as claimed. □

Claim
If T is any set of primes then there is a subring $\mathbf{R}$ of the ring of rational numbers so that $\mathsf{P}(\mathbf{R}) = T$.

This claim asserts that P maps the collection of subrings of the ring of rationals onto the collection of sets of primes. To prove this we have to come up with the subring $\mathbf{R}$. So let R be the set resulting closing the set

$$\{0, 1\} \cup \left\{ \frac{1}{p} \mid p \in T \right\}$$

by repeatedly using the operations $+, \cdot$, and $-$. This produces the set

$$R = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b > 0, \text{ and every prime factor of } b \text{ belongs to } T \right\}.$$

It is by now a routine matter to check that R is closed under all the operations. I do it just for $+$, which is the hardest of the operations. So suppose $\frac{a}{b}, \frac{c}{d} \in R$. Then all the primes factors of b and of d belong to T. But

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

Now a prime number p divides bd if and only if p divides at least one of b and d. So in any event if p is a prime dividing bd, then $p \in T$. This means

$$\frac{a}{b} + \frac{c}{d} \in R.$$

We could denote this ring $\mathbf{R}$ that was made from the set T of primes by $\mathsf{R}(T)$.

What is $\mathsf{P}(\mathbf{R})$? Well, for any prime p

$$\begin{aligned} p \in \mathsf{P}(\mathbf{R}) &\text{ if and only if } \frac{1}{p} \in R \\ &\text{if and only if every prime factor of } p \text{ belongs to } T \\ &\text{if and only if } p \in T \end{aligned}$$

This means $\mathsf{P}(\mathbf{R}) = T$, as desired, establishing the claim. □

We have just shown that $\mathsf{P}(\mathsf{R}(T)) = T$ for every set T of primes and it is possible to show that $\mathsf{R}(\mathsf{P}(\mathbf{R})) = \mathbf{R}$ for every subring $\mathbf{R}$ of the ring of rational numbers. That is, the functions P and R are inverses of each other.

It is even possible (and not too hard) to show that P preserves the ordering by set inclusion in the sense that for any subrings $\mathbf{R}$ and $\mathbf{S}$ of the ring of rational numbers

$$R \subseteq S \text{ if and only if } \mathsf{P}(\mathbf{R}) \subseteq \mathsf{P}(\mathbf{S}).$$

This seems like a satisfactory answer to the question of describing all the subrings of the ring of rational numbers. **Given any set T of primes we get a subring $\mathsf{R}(T)$ of the rationals and all the subrings of the rationals come up in this way.**