Problem 5

Let's consider all the numbers that are the sum of a rational and a rational mulitple of $\sqrt{2}$. In other words, let's define

$$\mathbb{Q}[\sqrt{2}] = \{r + s\sqrt{2} : r, s \in \mathbb{Q}\}$$

In this quesiton you'll prove that this is a field (using the usual notions of addition and multiplication). You may assume that $\mathbb{R}$ is a field (as will be our standard assumption from now on).

a) Check that addition and multiplication of elements of $\mathbb{Q}[\sqrt{2}]$ results in other elements of $\mathbb{Q}[\sqrt{2}]$. This tells us that we can do arithmetic with things of this form and always end up with things of this form.

Let's assume that there exists some elements p and $q \in \mathbb{Q}[\sqrt{2}]$. If we prove that both $p+q \in \mathbb{Q}[\sqrt{2}]$ and $pq \in \mathbb{Q}[\sqrt{2}]$, then we know $\mathbb{Q}[\sqrt{2}]$ is closed under both addition and multiplication.

$$(1) \quad (r_p + s_p\sqrt{2}) + (r_q + s_q\sqrt{2}) \quad (r_p + s_p\sqrt{2})(r_q + s_q\sqrt{2}) \quad (2)$$

Let's first take a look at addition, denoted by equation (1):

$$(r_p + s_p\sqrt{2} + r_q + s_q\sqrt{2})$$
$$(r_p + r_q + s_p\sqrt{2} + s_q\sqrt{2})$$
$$(r_p + r_q) + (s_p\sqrt{2} + s_q\sqrt{2})$$
$$(r_p + r_q) + ((s_p + s_q)\sqrt{2})$$

Now let's say there exists another element $t \in \mathbb{Q}[\sqrt{2}]$. We can redefine $(r_p + r_q)$ to equal r_t because according to the rules of addition in $\mathbb{R}$, when $p \in \mathbb{R}$ and $q \in \mathbb{R}$, then $(p+q) \in \mathbb{R}$. By the same notion, $(s_p + s_q)$ to equal t_s. Therefore, $\mathbb{Q}[\sqrt{2}]$ is closed under addition.

Next let's look at multiplication, denoted by equation (2):

$$(r_p + s_p\sqrt{2})(r_q + s_q\sqrt{2})$$
$$(r_p)(r_q) + (r_q)(s_p\sqrt{2}) + (r_p)(s_q\sqrt{2}) + 2(s_q)(s_p)$$
$$(r_p r_q) + ((r_q s_p)\sqrt{2}) + ((r_p s_q)\sqrt{2}) + (2 s_q s_p)$$
$$(r_p r_q) + (((r_q s_p) + (r_p s_q))\sqrt{2}) + (2 s_q s_p)$$
$$(r_p r_q) + (((r_q s_p) + (r_p s_q))\sqrt{2})\sqrt{2})$$
$$(r_p r_q + 2 s_q s_p) + (((r_q s_p) + (r_p s_q))\sqrt{2})$$

Just as we saw with addition, we can redefine $(r_p r_q + 2 s_q s_p)$ and $((r_q s_p) + (r_p s_q))$ which will both still be in $\mathbb{Q}[\sqrt{2}]$. Therefore, $\mathbb{Q}[\sqrt{2}]$ is closed under multiplication.

b) Check that negatives and reciprocals of elements of $\mathbb{Q}[\sqrt{2}]$ are in $\mathbb{Q}[\sqrt{2}]$.

Let's assume that there exists some element $p \in \mathbb{Q}[\sqrt{2}]$. If we prove that both $-p \in \mathbb{Q}[\sqrt{2}]$ and $p^{-1} \in \mathbb{Q}[\sqrt{2}]$, then we know $\mathbb{Q}[\sqrt{2}]$ is closed to both the negative and inverse of elements in $\mathbb{Q}[\sqrt{2}]$.

$$(1) \quad -(r_p + s_p\sqrt{2}) \quad (r_p + s_p\sqrt{2})^{-1} \quad (2)$$

Let's first take a look at negation, denoted by equation (1):

$$(-1)(r_p + s_p\sqrt{2})$$
$$(-1)(r_p) + (-1)(s_p\sqrt{2})$$
$$(-r_p) + ((-s_p)\sqrt{2})$$

Now let's say there exists another element $q \in \mathbb{Q}[\sqrt{2}]$. We can redefine $(-r_p)$ to equal r_q. By the same notion, $(-s_p)$ can be redefined to q_s. $r_q + s_q\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$.

Next let's look at reciprocal, denoted by equation (2). Note, $p^{-1} = 1/p$. Additionally, we can multiply by the opposite reciprocal in order to split the numerator with a common denominator.

$$(r_p + s_p\sqrt{2})^{-1}$$
$$\frac{1}{(r_p+s_p\sqrt{2})}$$
$$\frac{1}{(r_p+s_p\sqrt{2})} \cdot \frac{r_p-s_p\sqrt{2}}{r_p-s_p\sqrt{2}}$$
$$\frac{r_p-s_p\sqrt{2}}{r_p^2-2s_p^2}$$
$$\frac{r_p}{r_p^2-2s_p^2} - \frac{s_p\sqrt{2}}{r_p^2-2s_p^2}$$
$$\frac{r_p}{r_p^2-2s_p^2} + \frac{s_p}{2s_p^2-r_p^2}\sqrt{2}$$

Like with each of the situations before, we can redefine $\frac{r_p}{r_p^2-2s_p^2}$ and $\frac{s_p}{2s_p^2-r_p^2}$ to be r_q and s_q respectively. Both will still be in $\mathbb{Q}[\sqrt{2}]$. Therefore, the reciprocal is closed in $\mathbb{Q}[\sqrt{2}]$.

c) Explain briefly why axioms, such as A1, whose quantifiers are purely "$\forall$" are automaticly true for $\mathbb{Q}[\sqrt{2}]$ since they are true for $\mathbb{R}$. Pick out which axioms this argument works for.

For $\mathbb{Q}[\sqrt{2}]$ to be a field, it must be a set together with two binary operations called *addition* and *multiplication* that satisfies the 11 axioms as previously defined. The axioms containing "$\forall x$"as defined in $\mathbb{R}$ automatically hold "$\forall$" in $\mathbb{Q}[\sqrt{2}]$ because any subset of $\mathbb{Q}$ is also a subset of $\mathbb{R}$ since $\mathbb{Q} \subset \mathbb{R}$. However, some of the axioms contain "$\exists x$" in them, which do not automatically extend to $\mathbb{Q}[\sqrt{2}]$ because although $\mathbb{Q} \subset \mathbb{R}$, $\mathbb{Q} \not\subset \mathbb{R}$. Such axioms are A2, A3, A7, A8, A11. Therefore, there will be some elements of $\mathbb{R}$ that do not exist in $\mathbb{Q}$. Those axioms must therefore be proved. Such axioms are A1, A4, A5, A6, A9, and A10.

d) Prove that $\mathbb{Q}[\sqrt{2}]$ is a field, using your results from earlier parts.

As stated in part (c), the axioms that do not automatically hold for $\mathbb{Q}[\sqrt{2}]$ are A1, A4, A5, A6, A9, and A10. In part (a), we proved that there was closure under addition and multiplication, satisfying axioms A1 and A6. In part (b), we proved the existence of both additive and multiplicative inverses, satisfying axioms A5 and A10. The only ones left to prove are A4 and A9.

To prove A4, we need to show there exists an additive identity such that $\forall a \in \mathbb{F}$, $a + 0 = a$ In this case, we can redefine $r + s\sqrt{2}$ as a.

$$(r + s\sqrt{2}) + 0 = (r + s\sqrt{2})$$
$$((r + s\sqrt{2}) + (-(r + s\sqrt{2}))) + 0 = (r + s\sqrt{2}) + (-(r + s\sqrt{2})))$$

From here, we can use the A5 (since we proved it in part (b)), which states the existance of an additive inverse such that $a + (-a) = 0$. We redefined $(r + s\sqrt{2})$ as a, so we know the above equation implifies to $0 = 0$. Thus, Axiom A4 holds.

To prove A9, we need to show there exists an multiplicative identity such that $\forall a \in \mathbb{F}$, with $a \neq 0$, $a \cdot 1 = a$. Again, we can redefine $r + s\sqrt{2}$ as a.

$$1 \cdot (r + s\sqrt{2}) = (r + s\sqrt{2})$$

From here, we can use the A10 (since we proved it in part (b)), which states the existance of an multiplicative inverse. We redefined $(r + s\sqrt{2})$ as a, so we know the above equation implifies to $1 = 1$. Thus, Axiom A9 holds.

We have now proved that all 11 axioms hold for $\mathbb{Q}[\sqrt{2}]$ under the binary operations of *addition* and *multiplication*. Thus, $\mathbb{Q}[\sqrt{2}]$ is a field.