MA347 – HW22

Jonathan Lam

April 26, 2021

1. Prove that $\mathbb{Q}[\sqrt{2}] = \{a + \sqrt{2}b : a, b \in \mathbb{Q}\}$ is an integral domain.

   To show this, we must first show that $R = \mathbb{Q}[\sqrt{2}]$ is a ring, and then that it is a commutative ring with identity, and then that it has no zero divisors.

   Proof. (R is a ring.) Let $a = a_1 + \sqrt{2}a_2, b = b_1 + \sqrt{2}b_2 \in R$, for $a_1, a_2, b_1, b_2 \in \mathbb{Q}$. Define the sum element-wise. Define the product by

   $$\cdot(a, b) = ab = (a_1b_1 + 2a_2b_2) + \sqrt{2}(a_1b_2 + a_2b_1)$$

   Due to the closure of $\mathbb{Q}$ over product, $(a_1b_1 + 2a_2b_2), (a_1b_2 + a_2b_1) \in R$, so $ab \in R$.

   R1 $(R, +)$ is an abelian group due to the commutativity of the addition of rational numbers. (Proof not shown here b/c trivial.)

   R2 Let $a = a_1+\sqrt{2}a_2, b = b_1+\sqrt{2}b_2, c = c_1+\sqrt{2}c_2 \in R$, for $a_1, a_2, b_1, b_2, c_1, c_2 \in \mathbb{Q}$. Then:

   $$\begin{aligned}(ab)c &= ((a_1b_1 + 2a_2b_2) + \sqrt{2}(a_1b_2 + a_2b_1))c \\ &= ((a_1b_1 + 2a_2b_2)(c_1) + 2(a_1b_2 + a_2b_1)(c_2)) \\ &\quad + \sqrt{2}((a_1b_1 + 2a_2b_2)(c_2) + (a_1b_2 + a_2b_1)(c_1)) \\ &= (a_1(b_1c_1 + 2b_2c_2) + 2a_2(b_1c_2 + b_2c_1)) \\ &\quad + \sqrt{2}(a_1(b_1c_2 + b_2c_1) + a_2(b_1c_1 + 2b_2c_2)) \\ &= a((b_1c_1 + 2b_2c_2) + \sqrt{2}(b_1c_2 + b_2c_1)) \\ &= a(bc)\end{aligned}$$

   $\therefore$ product is associative.

R3 Let $a, b, c \in R$ as above. Then:

$$\begin{aligned}
a(b+c) &= a((b_1+c_1)+\sqrt{2}(b_2+c_2)) \\
&= (a_1(b_1+c_1)+2a_2(b_2+c_2)) \\
&\quad + \sqrt{2}(a_1(b_2+c_2)+a_2(b_1+c_1)) \\
&= ((a_1b_1+2a_2b_2)+(a_1c_1+2a_2c_2)) \\
&\quad + \sqrt{2}((a_1b_2+a_2b_1)+(a_1c_2+a_2c_1)) \\
&= ((a_1b_1+2a_2b_2)+\sqrt{2}(a_1b_2+a_2b_1)) \\
&\quad + ((a_1c_2+a_2c_1)+\sqrt{2}(a_1c_2+a_2c_1)) \\
&= ab+ac
\end{aligned}$$

(The proof of right distributivity follows likewise due to the commutativity and distributivity of $\mathbb{Q}$.)
$\therefore$ addition distributes over product.

R1, **R2**, **R3** are satisfied $\therefore R$ is a ring.

(Show that R is commutative and unital.) Use the commutativity of sum and product in $\mathbb{Q}$ to show that product in R is commutative. Assume $a, b \in R$ as previously:

$$\begin{aligned}
ab &= (a_1b_1+2a_2b_2)+\sqrt{2}(a_1b_2+a_2b_1) \\
&= (b_1a_1+2b_2a_2)+\sqrt{2}(b_2a_1+b_1a_2) \\
&= (b_1a_1+2b_2a_2)+\sqrt{2}(b_1a_2+b_2a_1) \\
&= ba
\end{aligned}$$

R has identity $e = 1+\sqrt{2}(0)$, because $\forall a \in R$:

$$ea = (1a_1+2(0)a_2)+\sqrt{2}(1a_2+0a_1) = a_1+\sqrt{2}a_2 = a$$

and $ea = a = ae$ because R is commutative.

(Show that R has no zero divisors.) Assume $ab = 0 = 0+\sqrt{2}(0)$ for some $a, b \in R$ and a nonzero.

$$(a_1b_1+2a_2b_2)+\sqrt{2}(a_1b_2+a_2b_1) = 0+\sqrt{2}(0) \Rightarrow \begin{cases} a_1b_1+2a_2b_2 = 0 \\ a_1b_2+a_2b_1 = 0 \end{cases}$$

$a \neq 0 \Rightarrow a_1, a_2$ are not both zero. Assume $a_1, b_1, b_2 \neq 0$ (i.e., $b \neq 0$). Then:

$$b_1 = -\frac{2a_2b_2}{a_1}, \quad b_2 = -\frac{a_2b_1}{a_1}$$
$$\Rightarrow b_1 = \frac{2a_2^2}{a_1^2}b_1 \Rightarrow \frac{2a_2^2}{a_1^2} = 1 \Rightarrow \frac{a_2}{a_1} = \frac{1}{\sqrt{2}} \Rightarrow a_2 = \frac{1}{\sqrt{2}}a_1$$

which is a contradiction since $a_2 = \frac{1}{\sqrt{2}} a_1 \notin \mathbb{Q}$. Thus $a_1 \neq 0 \Rightarrow b = 0$.

Similarly, if we assume that $a_2, b_1, b_2 \neq 0$ (i.e., $b \neq 0$), then:

$$b_2 = -\frac{a_1 b_1}{2a_2}, \quad b_1 = -\frac{a_1 b_2}{a_2}$$
$$\Rightarrow b_2 = \frac{a_1^2}{2a_2^2} b_2 \Rightarrow \frac{a_1^2}{2a_2^2} = 1 \Rightarrow \frac{a_1}{a_2} = \sqrt{2} \Rightarrow a_1 = \sqrt{2} a_2$$

which is again a contradiction because $\sqrt{2} \notin \mathbb{Q}$.

$\therefore\ ab = 0, a \neq 0 \Rightarrow b = 0$. (Similarly, $b \neq 0 \Rightarrow a = 0$ because R is commutative.) Thus R has no zero divisors. □

2. Let R be a commutative ring with identity. Let L, M, and N be (two-sided) ideals. Prove that:

   (a) $M + N$ is a left ideal of R.

   Proof. Let $x = m_1 + n_1 \in M + N$ and $r \in R$, for $m_1, m_2 \in M, n_1, n_2 \in N$. Then:

$$\begin{aligned} x + y &= (m_1 + n_1) + (m_2 + n_2) \\ &= (m_1 + m_2) + (n_1 + n_2) \\ &= m_3 + n_3 \in M + N \end{aligned}$$

   for $m_3 \in M, n_3 \in N$, since M, N are ideals and thus closed over addition. $\therefore M + N$ is closed over addition. We also have:

$$\begin{aligned} rx &= r(m_1 + n_1) \\ &= rm_1 + rn_2 \\ &= m_4 + n_4 \in M + N \end{aligned}$$

   for $m_4 \in M, n_4 \in N$, since M, N are ideals and closed over product with an element of R. $\therefore M + N$ is closed over product with an element of r.

   $\therefore M + N$ is a left ideal. (It is also a right ideal by the symmetric argument.) □

   (b) $L(M + N) = LM + LN$

   Proof. Let $l \in L, m \in M, n \in N$. By definition of product of ideals:

$$\begin{aligned} LM + LN &= \left\{ \sum_{i=1}^{s} l_i m_i : l_i \in L, m_i \in M, s \in \mathbb{Z}^+ \right\} \\ &\quad + \left\{ \sum_{i=1}^{t} l_i n_i : l_i \in L, n_i \in N, t \in \mathbb{Z}^+ \right\} \\ &= \left\{ \sum_{i=1}^{u} l_i m_i + l_i n_i : l_i \in L, m_i \in M, n_i \in N, u \in \mathbb{Z}^+ \right\} \\ &= \left\{ \sum_{i=1}^{u} l_i (m_i + n_i) : l_i \in L, m_i \in M, n_i \in N, u \in \mathbb{Z}^+ \right\} \\ &= L(M + N) \end{aligned}$$

   (Note that when we move from the two summations with upper limits s and t to the single summation with upper limit u, we "fill in" the missing terms with 0's, since $0 \in M, N$.) □

(c) $LM \subseteq L \cap M$

Proof. Let $x = lm \in LM$, $l \in L, m \in M$. By definition of the product of ideals:

$$LM = \left\{ \sum_{i=1}^{n} l_i m_i : l_i \in L, m_i \in M, n \in \mathbb{Z}^+ \right\}$$

Since L is a right ideal, each term $l_i m_i \in L$, and the linear combination lies in L. Similarly, since M is a left ideal, each term $l_i m_i \in M$, and the linear combination lies in M. Thus the linear combination lies in $L \cap M$, so $LM \subseteq L \cap M$. ☐