MAT401 - ASSIGNMENT 1 SOLUTIONS

Exercise 12-2

Observe that

$$\begin{aligned} 0 \times 6 &\equiv & 0 &\equiv & 0 (\text{mod } 10) \\ 2 \times 6 &\equiv & 12 &\equiv & 2 (\text{mod } 10) \\ 4 \times 6 &\equiv & 24 &\equiv & 4 (\text{mod } 10) \\ 6 \times 6 &\equiv & 36 &\equiv & 6 (\text{mod } 10) \\ 8 \times 6 &\equiv & 48 &\equiv & 8 (\text{mod } 10) \end{aligned}$$

Therefore the unity is 6. $\square$

Exercise 12-13

All subrings of $\mathbb{Z}$ can be expressed in the form $n\mathbb{Z}$ for some non-negative $n \in \mathbb{Z}$. From the textbook (pg 239, example 10) we know that $n\mathbb{Z}$ is a subring of $\mathbb{Z}$. Suppose R is a subring of $\mathbb{Z}$. If R contains only 0, then it is the same as $0\mathbb{Z}$. So suppose R contains at least one non-zero elements. Let $g = gcd(R)$ be the greatest integer dividing all non-zero elements of R. We know $g \in R$, since the greatest common divisor of any set of numbers can be constructed by summing multiples of the elements of R. Since g generates $g\mathbb{Z}$, we can conclude that $g\mathbb{Z}$ is a subring of R. Now suppose $\exists r \in R$ such that $r \notin g\mathbb{Z}$. This means that $\forall x \in \mathbb{Z}, x \times g \neq r \Rightarrow g \nmid r$, which contradicts the definition of g as the greatest common divisor. Thus R is a subring of $g\mathbb{Z}$, and $R = g\mathbb{Z}$. $\square$

Exercise 12-19

Denote the centre of a ring R as $Z(R) = \{x \in R \mid ax = xa, \forall a \in R\}$. Since $\forall a \in R, a0 = 0a$, $0 \in Z(R)$ and thus $Z(R)$ is non-empty. Let $u, v \in Z(R)$ be arbitrary. Then $\forall a \in R$, $au = ua$ and $av = va$. So $(u - v)a = ua - va = au - av = a(u - v)$, and thus $u - v \in Z(R)$. Also, $(uv)a = u(va) = u(av) = (ua)v = (au)v = a(uv)$, so $uv \in Z(R)$. Therefore, by the subring test, $Z(R)$ is a subring of R. $\square$

Exercise 12-22

Denote the unity in R as I_R. To show that $U(R)$ is a group under the multiplication operator in R, we will show that it satisfies the four properties of a group.

Identity $I_R \times I_R = I_R$, so $I_R \in U(R)$. Since $\forall r \in U(R), r \times I_R = r$, I_R is the identity in $U(R)$.

Inverse Suppose $a \in U(R)$. Then $\exists a^{-1} \in R$ such that $a \times a^{-1} = a^{-1} \times a = I_R$. So $a^{-1} \in U(R)$, and thus every element has an inverse.

Closure Suppose $a, b \in U(R)$. Then were know $\exists a^{-1}, b^{-1} \in U(R)$ such that $a \times a^{-1} = I_R$ and $b \times b^{-1} = I_R$. Since R is closed under multiplication, we know that $a \times b, b^{-1} \times a^{-1} \in R$. So $(a \times b) \times (b^{-1} \times a^{-1}) = a \times (b \times b^{-1}) \times a^{-1} = a \times a^{-1} = I_R$. Thus $a \times b$ has an inverse in R, and is therefore in $U(R)$. Therefore $U(R)$ is closed under multiplication.

Associativity Since R is a ring, we know that $\forall a, b, c \in R, (a \times b) \times c = a \times (b \times c)$, and thus $\forall a, b, c \in U(R), (a \times b) \times c = a \times (b \times c)$.

Therefore, $U(R)$ is a group under the multiplication of R. □

Exercise 13-13

Show that $\exists b \in R$ such that $(1 - a) \times b = 1$, where $a^n = 0$. Let $b = 1 + a + a^2 + \ldots + a^{n-2} + a^{n-1}$. Since R is closed under both $+$ and $\times$, $b \in R$. Computing $a \times b$ we get $a \times b = b - (a \times 1) - (a \times a) - \ldots - (a \times a^{n-1}) = b - (a + a^2 + \ldots + a^n) = 1 - a^n = 1 - 0 = 1$ (taking for granted associative and commutive properties of $+$). Thus b is the multiplicative inverse of $1 - a$. □

Exercise 13-24

Prove that $\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$, d a positive integer, is a field. If $\sqrt{d}$ is rational, then $\mathbb{Q}[\sqrt{d}] = \mathbb{Q}$, which is known to be a field. So assume $\sqrt{d} \notin \mathbb{Q}$.

First, we will show that $\mathbb{Q}[\sqrt{d}]$ is a ring. Let $a, b, c \in \mathbb{Q}[\sqrt{d}]$ with $a = a_0 + a1\sqrt{d}, b = b_0 + b1\sqrt{d}, c = c_0 + c1\sqrt{d}$. Then $a + b = (a_0 + b_0) + (a_1 + b_1)\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ and $ab = (a_0b_0 + a_1b_1d) + (a_0b_1 + b_0a_1)\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, so we are closed under addition and multiplication. Going through the six properties on page 235 of the text, and liberally using the fact that in $\mathbb{R}$ both $+$ and $\times$ are associative and commutative:

1 $a + b = (a_0 + b_0) + (a_1 + b_1)\sqrt{d} = (b_0 + a_0) + (b_1 + a_1)\sqrt{d} = b + a$.

2 $(a + b) + c = ((a_0 + b_0) + (a_1 + b_1)\sqrt{d}) + c = (a_0 + b_0 + c_0) + (a_1 + b_1 + c_1)\sqrt{d} = a + (b_0 + c_0) + (b_1 + c_1)\sqrt{d} = a + (b + c)$.

3 Let $0 = 0 + 0\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$. Then $a + 0 = (a_0 + 0) + (a_1 + 0)\sqrt{d} = a_0 + a_1\sqrt{d} = a$.

4 Let $-a = (-a_0) + (-a_1)\sqrt{d}$. Then $a + (-a) = (a_0 - a_0) + (a_1 - a_1)\sqrt{(d)} = 0 + 0\sqrt{d} = 0$.

5 $a(bc) = a((b_0c_0 + b_1c_1d) + (b_0c_1 + c_0b_1)\sqrt{d}) = (a_0b_0c_0 + a_1b_1c_0d + a_1b_0c_1d + a_0b_1c_1d) + (a_1b_0c_0 + a_0b_1c_0 + a_0b_0c_1 + a_1b_1c_1d)\sqrt{d} = ((a_0b_0 + a_1b_1d)c_0 + (a_0b_1 + b_0a_1)c_1d) + ((a_0b_0 + a_1b_1d)c_1 + c_0(a_0b_1 + b_0a_1))\sqrt{d} = ((a_0b_0 + a_1b_1d) + (a_0b_1 + b_0a_1)\sqrt{d})c = (ab)c$.

6.1 $a(b+c) = a((b_0+c_0)+(b_1+c_1)\sqrt{d}) = (a_0(b_0+c_0)+a_1(b_1+c_1)d)+(a_0(b_1+c_1)+(b_0+c_0)a_1)\sqrt{d} = ((a_0b_0+a_1b_1d)+(a_0c_0+a_1c_1d))+((a_0b_1+b_0a_1)+(a_0c_1+c_0a_1))\sqrt{d} = ab+ac$.

Before concluding with **6.2**, it will first be useful to show that $ab = ba$ (multiplication in $\mathbb{Q}[\sqrt{d}]$ is commutative). $ab = (a_0b_0+a_1b_1d)+(a_0b_1+b_0a_1)\sqrt{d} = (b_0a_0+b_1a_1d)+(b_0a_1+a_0b_1)\sqrt{d} = ba$. We are now one step closer to showing that $\mathbb{Q}[\sqrt{d}]$ is a field, and have greatly simplified the proof of **6.2**.

6.2 $(b+c)a = a(b+c) = ab+ac = ba+ca$.

Thus we have shown that $\mathbb{Q}[\sqrt{d}]$ is a commutative ring. Only two properties remain to make it a field.

$\mathbb{Q}[\sqrt{d}]$ **has a unity** Let $I_{\mathbb{Q}[\sqrt{d}]} = 1+0\sqrt{d}$. Then $aI_{\mathbb{Q}[\sqrt{d}]} = (a_01+a_10d)+(a_00+1a_1)\sqrt{d} = a_0+a1\sqrt{d} = a$. Thus $I_{\mathbb{Q}[\sqrt{d}]}$ is the unity in $\mathbb{Q}[\sqrt{d}]$.

Every non-zero element in $\mathbb{Q}[\sqrt{d}]$ **is a unit** Suppose $a \neq 0$. Clearly $a\frac{1}{a} = I_{\mathbb{Q}[\sqrt{d}]}$. So we need to show that for non-zero a, $\frac{1}{a_0+a_1\sqrt{d}} \in \mathbb{Q}[\sqrt{d}]$. $\frac{1}{a_0+a_1\sqrt{d}} = \frac{1}{a_0+a_1\sqrt{d}}\frac{a_0-a_1\sqrt{d}}{a_0-a_1\sqrt{d}} = \frac{a_0-a_1\sqrt{d}}{a_0^2-a_1^2d} = \frac{a_0}{a_0^2-a_1^2d} + \frac{-a_1}{a_0^2-a_1^2d}\sqrt{d}$ which is in $\mathbb{Q}[\sqrt{d}] \iff a_0^2-a_1^2d \neq 0$. But, $a_0^2-a_1^2d = 0 \iff a_0^2 = a_1^2d \iff a_0 = \pm a_1\sqrt{d}$. So either $a_0 = a_1 = 0$ (contradicting a non-zero) or $\frac{a_0}{\sqrt{d}} \in \mathbb{Q}$ (contradicting the assumption that $\sqrt{d}$ was irrational). Therefore $\frac{1}{a_0+a_1\sqrt{d}} \in \mathbb{Q}[\sqrt{d}]$, and thus every non-zero element of $\mathbb{Q}[\sqrt{d}]$ has a multiplicitive inverse.

Thus, $\mathbb{Q}[\sqrt{d}]$ is a commutative ring with unity in which every non-zero element is a unit, otherwise known as a field. $\square$