Name: Huize Shi - A92122910
Discussion: A04
Homework: 1

---

1. Suppose $R_1, \ldots, R_n$ are rings. Prove that $R_1, \ldots, R_n$ are unital if and only if $R_1 \times, \ldots, \times R_n$ is unital.

   Proof. (=>): Assume $R_1 \times, \ldots, \times R_n$ is unital, wants to show $R_1, \ldots, R_n$ are unital.

$$
\begin{aligned}
&R_1 \times, \ldots, \times R_n \text{ are unital } \Rightarrow \exists \text{ unity } (\mathbb{1}_1, \ldots, \mathbb{1}_n) \\
\Rightarrow &(\mathbb{1}_1, \ldots, \mathbb{1}_n) \cdot (r_1, \ldots, r_n) = (r_1, \ldots, r_n) \forall r_i \in R_i,\ i \in \mathbb{Z},\ 1 \leq i \leq n \\
\Rightarrow &(\mathbb{1}_1 \cdot r_1, \ldots, \mathbb{1}_n \cdot r_n) = (r_1, \ldots, r_n) \forall r_i \in R_i,\ i \in \mathbb{Z},\ 1 \leq i \leq n \\
\Rightarrow &(r_1, \ldots, r_n) \cdot (\mathbb{1}_1, \ldots, \mathbb{1}_n) = (r_1, \ldots, r_n) \forall r_i \in R_i,\ i \in \mathbb{Z},\ 1 \leq i \leq n \\
\Rightarrow &(r_1 \cdot \mathbb{1}_1, \ldots, r_n \cdot \mathbb{1}_n) = (r_1, \ldots, r_n) \forall r_i \in R_i,\ i \in \mathbb{Z},\ 1 \leq i \leq n \\
\Rightarrow &r_i \cdot \mathbb{1}_i = \mathbb{1}_i \cdot r_i = r_i,\ \forall r_i \in R_i,\ i \in \mathbb{Z},\ 1 \leq i \leq n
\end{aligned}
$$

   This shows that $\mathbb{1}_i$ is the unity for each ring R_i. Hence $R_1 \times, \ldots, \times R_n$ are unital rings.

   (<=): Assume $R_1, \ldots, R_n$ are unital, wants to show $R_1 \times, \ldots, \times R_n$ is unital. By assumption, $\exists\ \mathbb{1}_1 \ldots \mathbb{1}_n$, unity for each ring $R_1, \ldots, R_n$. Wants to show $(\mathbb{1}_1 \ldots \mathbb{1}_n)$ is the unity of $R_1 \times, \ldots, \times R_n$.

$$
\begin{aligned}
(\mathbb{1}_1, \ldots, \mathbb{1}_n) \cdot (r_1, \ldots, r_n) &= (\mathbb{1}_1 \cdot r_1, \ldots, \mathbb{1}_n \cdot r_n) \\
&= (r_1, \ldots, r_n) \forall r_i \in R_i,\ i \in \mathbb{Z},\ 1 \leq i \leq n
\end{aligned}
$$

$$
\begin{aligned}
(r_1, \ldots, r_n) \cdot (\mathbb{1}_1, \ldots, \mathbb{1}_n) &= (r_1 \cdot \mathbb{1}_1, \ldots, r_n \cdot \mathbb{1}_n) \\
&= (r_1, \ldots, r_n) \forall r_i \in R_i,\ i \in \mathbb{Z},\ 1 \leq i \leq n
\end{aligned}
$$

   Hence shown $(\mathbb{1}_1, \ldots, \mathbb{1}_n)$ is the unity of $R_1 \times, \ldots, \times R_n$. □

2. Suppose R is a unital ring. An element x of R is called a unit if it has a multiplicative inverse. Let $\mathcal{U}(R)$ be the set of all the units of R.

   (a) Prove that $\mathcal{U}(R)$ is closed under multiplication.
   Given $u_1, u_2 \in \mathcal{U}(R)$, wants to show $u_1 u_2 \in \mathcal{U}(R)$. Since $u_1, u_2 \in \mathcal{U}(R)$, $u_1^{-1}, u_2^{-1} \in \mathcal{U}(R)$. This means the inverse of $u_1 u_2$ exists $(u_1 u_2)^{-1} = u_2^{-1} u_1^{-1}$. This means that $u_1 u_2$ has multiplicative inverse, therefore in $\mathcal{U}(R)$. Hence shown $\mathcal{U}(R)$ is closed under multiplication.

   (b) Prove that $(\mathcal{U}(R), \cdot)$ is a group.

   Associativity $\cdot$ operator is associative by definition of ring.

Identity Since the ring is unital, and the inverse of the unity is itself, the unity is in $\mathcal{U}(R)$.

Inverse By the definition of $\mathcal{U}(R)$ all elements have inverse under multiplication.

(c) Suppose R_i are unital rings. Prove that $\mathcal{U}(R_1\times,\ldots,\times R_n) = \mathcal{U}(R_1)\times\cdots\times\mathcal{U}(R_n)$
Let r_i be any element in R_i where $i \in \mathbb{Z}, 1 \leq i \leq n$.

$$\mathcal{U}(R_1 \times \cdots \times R_n) = (u_1,\ldots,u_n) \text{ such that } \exists(u_1',\ldots,u_n'),$$
$$(u_1,\ldots,u_n)(u_1',\ldots,u_n') = (u_1',\ldots,u_n')(u_1,\ldots,u_n) = (\mathbb{1}_1,\ldots,\mathbb{1}_n)$$

By the definition of element wise multiplication:

$$(u_1,\ldots,u_n)(u_1',\ldots,u_n') = (u_1u_1',\ldots,u_nu_n') = (\mathbb{1}_1,\ldots,\mathbb{1}_n)$$
$$(u_1',\ldots,u_n')(u_1,\ldots,u_n) = (u_1'u_1,\ldots,u_n'u_n) = (\mathbb{1}_1,\ldots,\mathbb{1}_n)$$

This shows that each element u_i has multiplicative inverse. This means that u_i is in $\mathcal{U}(R)$. since u_i is a general term for $\mathcal{U}(R_i)$, this shows that $\mathcal{U}(R_1\times,\ldots,\times R_n) = \mathcal{U}(R_1)\times\cdots\times\mathcal{U}(R_n)$.

(d) Find $\mathcal{U}(\mathbb{Z}\times\mathbb{Q})$
By part c, $\mathcal{U}(\mathbb{Z}\times\mathbb{Q}) = \mathcal{U}(\mathbb{Z})\times\mathcal{U}(\mathbb{Q})$ Since the only integers with multiplicative inverse in $\mathbb{Z}$ are ±1, and $(Q,+,\cdot)$ is a field, $\mathcal{U}(\mathbb{Z}\times\mathbb{Q}) = (\pm1,\mathbb{Q})$

3. Show that $\{a+b\sqrt{3} \mid a,b\in\mathbb{Z}\}$ is ring.

Group portion First show $(\{a+b\sqrt{3} \mid a,b\in\mathbb{Z}\},+)$ is a abelian group.

Associativity

$$\begin{aligned}
&(a+b\sqrt{3}) + ((a'+b'\sqrt{3}) + (a''+b''\sqrt{3}))\\
=&(a+b\sqrt{3}) + (a'+b'\sqrt{3}) + (a''+b''\sqrt{3})\\
=&((a+b\sqrt{3}) + (a'+b'\sqrt{3})) + (a''+b''\sqrt{3})
\end{aligned}$$

Identity $0+0\sqrt{3}=0$, $0+a=a+0=a$. Identity exists in the set under $+$.

Inverse $(a+b\sqrt{3})^{-1} = -a-b\sqrt{3}$, since $a+b\sqrt{3}+(-a-b\sqrt{3}) = a-a+b\sqrt{3}-b\sqrt{3} = 0$. The inverse exists in the set under $+$.

Abelian $(a+b\sqrt{3})+(a'+b'\sqrt{3}) = a+b\sqrt{3}+a'+b'\sqrt{3} = a'+b'\sqrt{3}+a+b\sqrt{3} = (a'+b'\sqrt{3})+(a+b\sqrt{3})$. Hence shown the group is abelian.

Multiplication associativity

$$
\begin{aligned}
&(a+b\sqrt{3})\cdot((a'+b'\sqrt{3})\cdot(a''+b''\sqrt{3}))\\
=&(a+b\sqrt{3})\cdot(a'a''+a'b''\sqrt{3}+b'\sqrt{3}a''+b'\sqrt{3}b''\sqrt{3})\\
=&aa'a''+aa'b''\sqrt{3}+ab'\sqrt{3}a''+ab'\sqrt{3}b''\sqrt{3}\\
&+b\sqrt{3}a'a''+b\sqrt{3}a'b''\sqrt{3}+b\sqrt{3}b'\sqrt{3}a''+b\sqrt{3}b'\sqrt{3}b''\sqrt{3})\\
=&(aa'+ab'\sqrt{3}+b\sqrt{3}a'+b\sqrt{3}b'\sqrt{3})(a''+b''\sqrt{3})\\
=&((a+b\sqrt{3})\cdot(a'+b'\sqrt{3}))\cdot(a''+b''\sqrt{3})
\end{aligned}
$$

Distributive property

$$
\begin{aligned}
&(a+b\sqrt{3})\cdot((a'+b'\sqrt{3})+(a''+b''\sqrt{3}))\\
=&(a+b\sqrt{3})\cdot(a'+b'\sqrt{3}+a''+b''\sqrt{3})\\
=&aa'+ab'\sqrt{3}+aa''+b''\sqrt{3}+b\sqrt{3}a'+b\sqrt{3}b'\sqrt{3}+b\sqrt{3}a''+b''\sqrt{3}\\
=&(a+b\sqrt{3})\cdot(a'+b'\sqrt{3})+(a+b\sqrt{3})\cdot(a''+b''\sqrt{3})
\end{aligned}
$$

4. As in problem 3, one can show $F=\{a+b\sqrt{3}\mid a,b\in\mathbb{Q}\}$ is a ring. Show that $\mathcal{U}(F)=F\setminus\{0\}$; that means any non-zero element is a unit.

Proof. Given $a+b\sqrt{3}$, define $(a+b\sqrt{3})^{-1}$ as $\frac{a-b\sqrt{3}}{aa-3bb}$. Wants to show the inverse is an element of the ring.

$$
\begin{aligned}
(a+b\sqrt{3})\cdot\frac{a-b\sqrt{3}}{aa-3bb}&=\frac{a-b\sqrt{3}}{aa-3bb}\cdot(a+b\sqrt{3})=\frac{aa-3bb}{aa-3bb}=1\\
\frac{a-b\sqrt{3}}{aa-3bb}&=\frac{a}{aa-3bb}-\frac{b}{aa-3bb}\cdot\sqrt{3}
\end{aligned}
$$

This is of the form $a+b\sqrt{3}$ since $(\mathbb{Q},+,\cdot)$ is a field. It contains inverses for all elements and is closed under addition (denominators are therefore rational). Since $\mathbb{Q}$ is a field, $\frac{1}{aa-3bb}$ is rational since it is the multiplicative inverse of $aa-3bb$ which previously explained to be rational. Hence any non-zero element of F is a unit since $\frac{a-b\sqrt{3}}{aa-3bb}$ is demonstrated to be the multiplicative inverse of any element in F. □

5. For a ring R, let $R[x]=\{a_0+a_1x+\cdots+a_nx^n\mid a_0,\dots,a_n\in\mathcal{R},n\in\mathbb{Z}^{\geq 0}\}$ be the ring of polynomials with coefficients in R and indeterminant x. We add and multiply polynomials as usual.

(a) Show that $\mathcal{U}(\mathbb{Z}[x]) = \{\pm 1\}$
Given $z_x = a_0 + a_1 x + \cdots + a_n x^n$, it's inverse $z_x^{-1} = a'_0 + a'_1 x + \cdots + a'_n x^n$.

$$z_x z'_x = \sum_{i=0}^{n} \sum_{j=0}^{n} a_i a'_j x^{i+j} = (1, 0, 0, \ldots 0)$$

Assume towards a contradiction that z_x and z'_x are not ± 1. This is impossible because the x terms cannot be cancled. Hence it can only be the case if the polynomial is $(1, 0, \ldots, 0)$ or $(-1, 0, \ldots, 0)$.

(b) Show that $2x + 1 \in \mathcal{U}(\mathbb{Z}_8[x])$
Define the multiplicative inverse of $(2x + 1)$ as $(2x + 1)^{-1} = \frac{1}{2x+1}$

6. Suppose A is a ring with unity 1. Suppose there is $a_0 \in A$ such that $a_0^2 = 1$. Let $B := \{a_0 r a_0 \mid r \in A\}$. Prove that B is a subring of A.

Subtraction Given any r and r' in A, consider $a_0 r a_0 - a_0 r' a_0$:

$$a_0 r a_0 - a_0 r' a_0 = a_0 (r - r') a_0$$

Since $r, r' \in A$, A is a ring, $r - r'$ is also in A. Hence the first condition is satisfied.

Multiplication Given any r and r' in A, consider $(a_0 r a_0) \cdot (a_0 r' a_0)$. Since multiplication is associative the following holds:

$$\begin{aligned}(a_0 r a_0) \cdot (a_0 r' a_0) &= a_0 r (a_0 \cdot a_0) r' a_0 \\ &= a_0 r \cdot 1 \cdot r' a_0 \\ &= a_0 r r' a_0\end{aligned}$$

Since $r, r' \in A$, A is a ring, rr' is also in A. Hence the second condition is satisfied.
Hence shown $B \leq A$.