Test 1 - Answers and Solutions

Question about course 1.

$(R, +, \times)$ is a ring if it satisfies each of the following point

a) $R$ is a nonempty set

b) $+$ and $\times$ are binary operations on $R$
   \[
   \forall a, b \in R, \begin{cases} a + b \in R \\ a \times b \in R \end{cases}
   \]

c) $(R, +)$ is an abelian group, that is it satisfies each of the following point
   
   c1) $\forall a, b, c \in R, (a + b) + c = a + (b + c)$
   
   c2) $\exists 0 \in R/ \forall a \in R, a + 0 = 0 + a = a$
   
   c3) $\forall a \in R, \exists (-a) \in R/ a + (-a) = (-a) + a = 0$
   
   c4) $\forall a, b \in R, a + b = b + a$


d) the binary operation $\times$ is associative
   \[
   \forall a, b, c \in R, (a \times b) \times c = a \times (b \times c)
   \]

e) the binary operation $\times$ is distributive over the binary operation $+$
   \[
   \forall a, b, c \in R, \begin{cases} a \times (b + c) = a \times b + a \times c \\ (b + c) \times a = b \times a + c \times a \end{cases}
   \]

Question about course 2.

$\varphi$ is an automorphism of the group $(G, \star)$ if it satisfies each of the following point

a) $\varphi$ is a map from $G$ into itself

b) $\varphi$ is a bijection

   b1) $\varphi$ is injective: $\forall a, b \in G, \varphi(a) = \varphi(b) \implies a = b$

   b2) $\varphi$ is surjective: $\forall a \in G, \exists b \in G/ \varphi(b) = a$

c) $\varphi$ is a group homomorphism: $\forall a, b \in G, \varphi(a \star b) = \varphi(a) \star \varphi(b)$

Exercise 3.

1. Let $a$ and $a'$ be two elements in $A$, namely $a = n + k\sqrt{5}$ and $a' = n' + k'\sqrt{5}$ where $n, k, n', k' \in \mathbb{Z}$. Then

   $a + (-a') = (n + k\sqrt{5}) - (n' + k'\sqrt{5}) = n + k\sqrt{5} - n' - k'\sqrt{5} = (n - n') + (k - k')\sqrt{5}$

Since $(n - n') \in \mathbb{Z}$ and $(k - k') \in \mathbb{Z}$, it follows that $a + (-a') \in A$. Consequently $(A, +)$ is a subgroup of $(\mathbb{R}, +)$.  

2. We need to prove that $\times$ is a binary operation on $A$, $\times$ is associative and $\times$ is distributive over $\cdot$.
Let $a$ and $a'$ be two elements in $A$, namely $a = n + k\sqrt{5}$ and $a' = n' + k'\sqrt{5}$ where $n, k, n', k' \in \mathbb{Z}$. Then

$$a \times a' = (n + k\sqrt{5}) \times (n' + k'\sqrt{5}) = nn' + nk'\sqrt{5} + nk\sqrt{5} + 5kk' = (nn' + 5kk') + (nk' + n'k)\sqrt{5}$$

Since $(nn' + 5kk') \in \mathbb{Z}$ and $(nk' + n'k) \in \mathbb{Z}$, it follows that $a \times a' \in A$. Consequently $\times$ is a binary operation on $A$.

Let $a, a'$ and $a''$ be three elements in $A$. Since $\times$ is associative on $\mathbb{R}$ and distributive over $\cdot$ on $\mathbb{R}$, we have

$$\begin{align*}
(a \times a') \times a'' &= a \times (a' \times a'') \\
(a \times a' + a \times a'') &= a \times a' + a \times a'' \\
(a' + a'') \times a &= a' \times a + a'' \times a
\end{align*}$$

Consequently $\times$ is associative on $A$ and distributive over $\cdot$ on $A$ as well.

**Exercise 4.** 1. Let $f$ and $g$ be two elements in $F_0$, that are two functions from $\mathbb{R}$ to itself such that $f(1) = g(1) = 0$. Then the function $(f + (-g)) : x \mapsto (f + (-g))(x) = f(x) - g(x)$ is from $\mathbb{R}$ to itself and $(f + (-g))(1) = f(1) - g(1) = 0 - 0 = 0$. Consequently $(f + (-g)) \in F_0$ and it follows that $(F_0, +)$ is a subgroup of $(F, +)$.

2. Let $f$ and $g$ be two elements in $F_1$, that are two functions from $\mathbb{R}$ to itself such that $f(1) = g(1) = 1$. Then the function $(f + g) : x \mapsto (f + g)(x) = f(x) + g(x)$ is from $\mathbb{R}$ to itself and $(f + g)(1) = f(1) + g(1) = 1 + 1 = 2 = 1$. Consequently $(f + g) \notin F_1$ and it follows that $\cdot$ is not a binary operation on $F_1$. Finally $(F_1, +)$ is not a group.

3. For every real number $x$, if $f$ and $g$ are two elements in $F_x$ then the function $(f + g)$ is in $F_{2x}$ (since $(f + g)(1) = f(1) + g(1) = x + x = 2x$). But $F_{2x}$ is disjoint from $F_x$ as soon as $x \neq 0$ (since $2x \neq x$). Therefore $\cdot$ is not a binary operation on $F_x$ for $x \neq 0$. Consequently $x = 0$ is the only real number such that $(F_x, +)$ is a group.

4. Let $f$ and $g$ be two elements in $F$, that are two function from $\mathbb{R}$ to itself. Then

$$\Phi(f + g) = (f + g)(1) = f(1) + g(1) = \Phi(f) + \Phi(g)$$

Consequently, $\Phi$ is a homomorphism from $(F, +)$ into $(\mathbb{R}, +)$.

**Exercise 5.**

1. $u_0 = 4^{3 \times 0 + 2} + 8^{2 \times 0 + 1} = 4^2 + 8 = 16 + 8 = 24 = 2 \times 9 + 6 = 6 \quad \text{[9]}$

2. $u_1 = 4^{3 \times 1 + 2} + 8^{2 \times 1 + 1} = 4^5 + 8^3$

Moreover

$$\begin{align*}
4^2 &= 4 \times 4 = 16 = 1 \times 9 + 7 \equiv 7 \quad \text{[9]} \\
4^3 &= 4^2 \times 4 = 7 \times 4 = 28 = 3 \times 9 + 1 \equiv 1 \quad \text{[9]} \\
4^5 &= 4^3 \times 4^2 = 1 \times 7 \equiv 7 \quad \text{[9]} \\
8^3 &= (2 \times 4)^3 = 2^3 \times 4^3 \equiv 8 \times 1 \equiv 8 \quad \text{[9]}
\end{align*}$$

So $u_1 = 4^5 + 8^3 \equiv 7 + 8 \equiv 15 \equiv 1 \times 9 + 6 \equiv 6 \quad \text{[9]}$

$u_2 = 4^{3 \times 2 + 2} + 8^{2 \times 2 + 1} = 4^6 + 8^5$

Moreover

$$\begin{align*}
4^5 &= 4^3 \times 4^2 \equiv 7 \times 1 \equiv 7 \quad \text{[9]} \\
8^5 &= (2 \times 4)^5 = 2^5 \times 4^5 \equiv 32 \times 7 \equiv 5 \times 7 \equiv 35 \equiv 8 \quad \text{[9]}
\end{align*}$$

(since $32 = 3 \times 9 + 5 \equiv 5$ [9] and $35 = 3 \times 9 + 8 \equiv 8$ [9])

So $u_2 = 4^8 + 8^5 \equiv 7 + 8 \equiv 15 \equiv 1 \times 9 + 6 \equiv 6 \quad \text{[9]}$
3. \( u_{n+1} = 4^{3(n+1)+2} + 8^{2(n+1)+1} = 4^{3n+2} + 8^{2n+1} = 4^3 \times 4^{3n+2} + 8^2 \times 8^{2n+1} \)

Moreover
\[
\begin{cases}
4^3 \equiv 1 \pmod{9} \\
8^2 = 8 \times 8 = 64 = 7 \times 9 + 1 \equiv 1 \pmod{9}
\end{cases}
\]

So \( u_{n+1} = 4^3 \times 4^{3n+2} + 8^2 \times 8^{2n+1} \equiv 1 \times 4^{3n+2} + 1 \times 8^{2n+1} \equiv 4^{n+2} + 8^{n+1} \equiv u_n \pmod{9} \)

In particular the assumption \( u_n \equiv 6 \pmod{9} \) implies that \( u_{n+1} \equiv 6 \pmod{9} \).

4. It follows by induction that \( u_n \equiv 6 \pmod{9} \) for every \( n \in \mathbb{N} \).

Exercise 6.

1. Since 13 is a prime number, every element in \( \mathbb{Z}/13\mathbb{Z} \) distinct from 0 has an inverse element for the multiplication. It follows that \((\mathbb{Z}/13\mathbb{Z} - \{0\}, \times)\) is a group.

2. We have
\[
\begin{align*}
0 \times 6 & = 0 \equiv 0 \pmod{13} \\
1 \times 6 & = 6 \equiv 6 \pmod{13} \\
2 \times 6 & = 12 \equiv 12 \pmod{13} \\
3 \times 6 & = 18 = 1 \times 13 + 5 \equiv 5 \pmod{13} \\
4 \times 6 & = 24 = 1 \times 13 + 11 \equiv 11 \pmod{13} \\
5 \times 6 & = 30 = 2 \times 13 + 4 \equiv 4 \pmod{13} \\
6 \times 6 & = 36 = 2 \times 13 + 10 \equiv 10 \pmod{13}
\end{align*}
\]

and
\[
\begin{align*}
7 \times 6 & = 42 = 3 \times 13 + 3 \equiv 3 \pmod{13} \\
8 \times 6 & = 48 = 3 \times 13 + 9 \equiv 9 \pmod{13} \\
9 \times 6 & = 54 = 4 \times 13 + 2 \equiv 2 \pmod{13} \\
10 \times 6 & = 60 = 4 \times 13 + 8 \equiv 8 \pmod{13} \\
11 \times 6 & = 66 = 5 \times 13 + 1 \equiv 1 \pmod{13} \\
12 \times 6 & = 72 = 5 \times 13 + 7 \equiv 7 \pmod{13}
\end{align*}
\]

So \( y = \prod \) answers the question (\( \prod \times 6 = 1 \) since \( 11 \times 6 \equiv 1 \pmod{13} \)).

3. At first, since \((\mathbb{Z}/13\mathbb{Z}, +)\) is a group, \((E)\) is equivalent to
\[
(E) \quad 6 \times x = 2 - 7 = 2 - 7 = -5 = -1 \times 13 + 8 = 8
\]

By multiplying both sides of \((E)\) with \( \prod \), we get
\[
\begin{align*}
\prod \times (6 \times x) &= \prod \times 8 \\
(\prod \times 6) \times x &= \prod \times 8 \quad \text{(by using associativity of \( \times \))} \\
\overline{1} \times x &= 88 \quad \text{(from the result of the previous question)} \\
x &= 6 \times 13 + 10 \quad \text{(since \( \overline{1} \) is the identity element for \( \times \))} \\
x &= 10
\end{align*}
\]

Finally \((E)\) has an unique solution in \( \mathbb{Z}/13\mathbb{Z} \) which is \( x = \overline{10} \).

4. Since 11 is a prime number, every element in \( \mathbb{Z}/11\mathbb{Z} \) distinct from 0 has an inverse element for the multiplication. In particular \( \overline{2} \times \overline{6} = 2 \times 6 = 12 = 1 \times 11 + 1 = \overline{1} \). Therefore we get in \( \mathbb{Z}/11\mathbb{Z} \)
\[
\begin{align*}
(E) \quad 2 \times (6 \times x) &= 2 \times (\overline{2} - 7) \\
(2 \times 6) \times x &= 2 \times -\overline{5} \\
\overline{1} \times x &= -\overline{10} \\
x &= -1 \times 11 + 1 \\
x &= \overline{1}
\end{align*}
\]

Consequently \((E)\) has an unique solution in \( \mathbb{Z}/11\mathbb{Z} \) which is \( x = \overline{1} \).