Solutions to Exercise #7

(範圍: Rings, Groups)

1. Prove (b) and (e) of the theorem in page 142 of lecture notes. (15%)

Sol: (b) Suppose that x and y are two inverses of $a \in G$.

Then, $x = x \cdot e = x \cdot (a \cdot y) = (x \cdot a) \cdot y = e \cdot y = y$.

(e) (if part) $(a \cdot b)^2 = a^2 \cdot b^2 \Rightarrow (a \cdot b) \cdot (a \cdot b) = (a \cdot a) \cdot (b \cdot b)$

$$\Rightarrow a^{-1}(a \cdot b) \cdot (a \cdot b)\, b^{-1} = a^{-1}(a \cdot a) \cdot (b \cdot b)\, b^{-1}$$

$$\Rightarrow b \cdot a = a \cdot b.$$

(only if part) $(a \cdot b)^2 = (a \cdot b) \cdot (a \cdot b) = a \cdot (b \cdot a) \cdot b = a \cdot (a \cdot b) \cdot b$

$$= (a \cdot a) \cdot (b \cdot b) = a^2 \cdot b^2.$$

2. Prove the theorem in page 146 of lecture notes. (20%)

Sol: (closure) Suppose $(g_1, h_1), (g_2, h_2) \in G \times H$.

Then, $(g_1, h_1) \cdot (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2) \in G \times H$,

because $g_1 \circ g_2 \in G$ and $h_1 * h_2 \in H$.

(associativity) Suppose $(g_1, h_1), (g_2, h_2)$, $(g_3, h_3) \in G \times H$.

Then, $((g_1, h_1) \cdot (g_2, h_2)) \cdot (g_3, h_3) = (g_1 \circ g_2, h_1 * h_2) \cdot (g_3, h_3)$

$$= ((g_1 \circ g_2) \circ g_3, (h_1 * h_2) * h_3) = (g_1 \circ (g_2 \circ g_3), h_1 * (h_2 * h_3))$$

$$= (g_1, h_1) \cdot (g_2 \circ g_3, h_2 * h_3) = (g_1, h_1) \cdot ((g_2, h_2) \cdot (g_3, h_3)).$$

(identity) Suppose that e_G and e_H are the identities of G and H, respectively.

Then, (e_G, e_H) is the identity of $G \times H$.

(inverse) (g^{-1}, h^{-1}) is the inverse of $(g, h) \in G \times H$.

3. P. 685: 12 (only for (b)). (20%)

Sol: Suppose $A = \begin{bmatrix} 2a & 2b \\ 2c & 2d \end{bmatrix}$, $B = \begin{bmatrix} 2e & 2f \\ 2g & 2h \end{bmatrix} \in T$.

Then, $A + B = \begin{bmatrix} 2a+2e & 2b+2f \\ 2c+2g & 2d+2h \end{bmatrix} = \begin{bmatrix} 2(a+e) & 2(b+f) \\ 2(c+g) & 2(d+h) \end{bmatrix} \in T$,

$A \cdot B = \begin{bmatrix} 4ae+4bg & 4af+4bh \\ 4ce+4dg & 4cf+4dh \end{bmatrix} = \begin{bmatrix} 2(2ae+2bg) & 2(2af+2bh) \\ 2(2ce+2dg) & 2(2cf+2dh) \end{bmatrix} \in T$, and

$$-A = \begin{bmatrix} -2a & -2b \\ -2c & -2d \end{bmatrix} = \begin{bmatrix} 2(-a) & 2(-b) \\ 2(-c) & 2(-d) \end{bmatrix} \in T.$$

Therefore, T is a subring of $M_2(\mathbf{Z})$.

On the other hand, suppose $C = \begin{bmatrix} w & x \\ y & z \end{bmatrix} \in M_2(\mathbf{Z})$.

Then, $C \cdot A = \begin{bmatrix} w & x \\ y & z \end{bmatrix}\begin{bmatrix} 2a & 2b \\ 2c & 2d \end{bmatrix} = \begin{bmatrix} 2aw+2cx & 2bw+2dx \\ 2ay+2cz & 2by+2dz \end{bmatrix}$

$= \begin{bmatrix} 2(aw+cx) & 2(bw+dx) \\ 2(ay+cz) & 2(by+dz) \end{bmatrix} \in T$, and

$A \cdot C = \begin{bmatrix} 2a & 2b \\ 2c & 2d \end{bmatrix}\begin{bmatrix} w & x \\ y & z \end{bmatrix} = \begin{bmatrix} 2aw+2by & 2ax+2bz \\ 2cw+2dy & 2cx+2dz \end{bmatrix}$

$= \begin{bmatrix} 2(aw+by) & 2(ax+bz) \\ 2(cw+dy) & 2(cx+dz) \end{bmatrix} \in T.$

Therefore, T is an ideal of $M_2(Z)$.

4. Prove that in $\mathbf{Z}_n$, $[a]$ is a unit if and only if $\gcd(a, n) = 1$. (15%)

Sol: (if part) If $\gcd(a, n) = 1$, then $as + tn = 1$ for some integers s, t.
That is, $as \equiv 1 \pmod{n}$, or $[a] \cdot [s] = [1]$.
Hence, $[a]$ is a unit of $\mathbf{Z}_n$.

(only if part) If $[a]$ is a unit of $\mathbf{Z}_n$, then $[as] = [a] \cdot [s] = [1]$ for some $[s] \in \mathbf{Z}_n$.
So, $as = 1 + qn$, or $as + n(-q) = 1$, for some integer q.
Hence, $\gcd(a, n) = 1$.

5. P. 704: 4. (15%)

Sol: Define f: $\mathbf{R} \to S$ by $f(r) = \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix}$, for each $r \in \mathbf{R}$.

Then, f is one-to-one and onto.

For all $r, s \in \mathbf{R}$,

$f(r+s) = \begin{bmatrix} r+s & 0 \\ 0 & r+s \end{bmatrix} = \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix} + \begin{bmatrix} s & 0 \\ 0 & s \end{bmatrix} = f(r) + f(s)$, and

$$f(r \cdot s) = \begin{bmatrix} rs & 0 \\ 0 & rs \end{bmatrix} = \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix} \cdot \begin{bmatrix} s & 0 \\ 0 & s \end{bmatrix} = f(r) \cdot f(s).$$

Therefore, f is a ring isomorphism and $\mathbf{R}$ is isomorphic to S.

6. Solve $x \equiv 8 \pmod{11}$, $x \equiv 9 \pmod{12}$, and $x \equiv 10 \pmod{13}$. (15%)

Sol. $(a_1, a_2, a_3) = (8, 9, 10)$; $(m_1, m_2, m_3) = (11, 12, 13)$;
$(M_1, M_2, M_3) = (156, 143, 132)$.

$M_1 x_1 \equiv 1 \pmod{m_1} \Rightarrow [x_1] = [M_1]^{-1} = [156]^{-1} = [2]^{-1} = [6]$ in $Z_{m_1} = Z_{11}$.

$M_2 x_2 \equiv 1 \pmod{m_2} \Rightarrow [x_2] = [M_2]^{-1} = [143]^{-1} = [11]^{-1} = [11]$ in $Z_{m_2} = Z_{12}$.

$M_3 x_3 \equiv 1 \pmod{m_3} \Rightarrow [x_3] = [M_3]^{-1} = [132]^{-1} = [2]^{-1} = [7]$ in $Z_{m_3} = Z_{13}$.

Then, $x = a_1 M_1 x_1 + a_2 M_2 x_2 + a_3 M_3 x_3 = 30885$, and $[x] = [30885] = [1713]$ in $Z_{11 \times 12 \times 13} = Z_{1716}$ is the solution.