Solutions to Examination #2

(範圍: Algebra)

1. Prove that if $3 \mid n^2$, then $3 \mid n$, where n is a positive integer, by the methods of
   (a) $p \to q \Leftrightarrow \neg q \to \neg p$; (5%)
   (b) contradiction. (5%)

Sol: (a) If $n = 3k + 1$, then $n^2 = (3k + 1)^2 = 3k' + 1$.
If $n = 3k + 2$, then $n^2 = (3k + 2)^2 = 3k' + 1$.

(b) Suppose $3 \mid n^2$ and $n = 3k + 1$.
$n = 3k + 1 \Rightarrow n^2 = (3k + 1)^2 = 3k' + 1$, a contradiction to $3 \mid n^2$.
Similarly, there is a contradiction, if $3 \mid n^2$ and $n = 3k + 2$.

2. Let $(K, \cdot, +)$ be a Boolean algebra. The following is a proof of $a \cdot (a + b) = a$ for every $a, b \in K$.

$$a \cdot (a + b) = (a \cdot a) + (a \cdot b) = a + (a \cdot b) = (a \cdot 1) + (a \cdot b)$$
$$= a \cdot (1 + b) = a \cdot 1 = a.$$

Please prove $a + (a \cdot b) = a$ for every $a, b \in K$. (10%)

Sol: $a + (a \cdot b) = (a + a) \cdot (a + b) = a \cdot (a + b) = (a + 0) \cdot (a + b) = a + 0 \cdot b = a + 0 = a$.

3. Is the following argument correct or wrong? Why? (10%)

Suppose that $\Re$ is a binary relation on a non-empty set A. If $\Re$ is symmetric and
transitive, then $\Re$ is reflexive.

Proof. Let $(x, y) \in \Re$. By the symmetric property, we have $(y, x) \in \Re$.
Then, with $(x, y), (y, x) \in \Re$, it follows by the transitive property that we have $(x, x) \in \Re$. As a consequence, $\Re$ is reflexive.

Sol. The argument is wrong, because there may exist $a \in A$ having $(a, b) \notin \Re$ for all $b \in A$.

4. Define $a \, R \, b$ if and only if $a \equiv b \pmod{n}$. Prove that R is an equivalence relation on Z. (10%)

Sol. We only need to show that R is reflexive, symmetric, and transitive.

- reflexive

  $\forall a \in Z,\ a \equiv a \pmod{n} \Rightarrow a\,R\,a$

- symmetric

  $$\begin{aligned}\forall a, b \in Z,\ a\,R\,b &\Rightarrow a \equiv b \pmod{n} \\ &\Rightarrow b \equiv a \pmod{n} \\ &\Rightarrow b\,R\,a\end{aligned}$$

- transitive

  $$\begin{aligned}\forall a, b, c \in Z,\ a\,R\,b \text{ and } b\,R\,c &\Rightarrow a \equiv b \pmod{n} \text{ and } b \equiv c \pmod{n} \\ &\Rightarrow a \equiv c \pmod{n} \\ &\Rightarrow a\,R\,c\end{aligned}$$

5. Suppose that $(R, +, \cdot)$ is a commutative ring with unity. Prove that R is an integral domain if and only if for $a, b, c \in R$ and $a \neq z$, $a \cdot b = a \cdot c \Rightarrow b = c$. (10%)

Sol. We only need to show no zero divisor $\Leftrightarrow$ the cancellation law of multiplication.

(if) Consider $a, b \in R$ with $a \cdot b = z$.
Assume $a \neq z$. Since $a \cdot b = z = a \cdot z$, we have $b = z$.
So, R has no zero divisor.

(only if) Consider $a, b, c \in R$, $a \neq z$, and $a \cdot b = a \cdot c$.

$$\begin{aligned}a \cdot b = a \cdot c &\Rightarrow a \cdot b + (-(a \cdot c)) = z \\ &\Rightarrow a \cdot (b + (-c)) = z \\ &\Rightarrow b + (-c) = z \\ &\Rightarrow b = -(-c) = c\end{aligned}$$

6. Define two binary operations $\oplus, \odot$ on Z as follows: $a \oplus b = a + b - 1$ and $a \odot b = a + b - ab$. Then, $(Z, \oplus, \odot)$ is a commutative ring with unity. Please find (1) the zero of Z; (2) the inverse of a under $\oplus$; (3) the unity of Z. (6%)
Also show that Z has no proper divisor of zero. (4%)

Sol. (1) 1. (2) $2 - a$. (3) 0.

Z has no proper divisor of zero, because

$$\begin{aligned}a \odot b = 1 &\Rightarrow a + b - ab = 1 \Rightarrow (a-1)(1-b) = 0 \\ &\Rightarrow a = 1 \text{ or } b = 1.\end{aligned}$$

7. Consider the ring $(Z, \oplus, \odot)$. Prove that for each integer $0 < a < n$, if $\gcd(a, n) > 1$, then $[a]$ is a proper zero divisor of Z_n. (10%)

Sol. Suppose $\gcd(a, n) = k > 1$. Then, $a = kx$ and $n = ky$, where $\gcd(x, y) = 1$.
Since $[a] \cdot [y] = [ay] = [kxy] = [xn] = [0]$, where $[a] \neq [0]$ and $[y] \neq [0]$,
$[a]$ is a proper zero divisor.

8. Let $f: (R, +, \cdot) \to (S, \oplus, \odot)$ be a ring homomorphism. Prove that if A is a subring of R, then $f(A)$ is a subring of S. (hints: you need to show the closure property and inverse property) (10%)

Sol. We only need to show $a \oplus b, a \odot b, -a \in f(A)$ for all $a, b \in f(A)$.
$a \oplus b = f(x) \oplus f(y) = f(x + y) \in f(A)$ (since $x + y \in A$)
$a \odot b = f(x) \odot f(y) = f(x \cdot y) \in f(A)$ (since $x \cdot y \in A$)
$-a = -f(x) = f(-x) \in f(A)$ (since $-x \in A$)

9. A positive integer solution for $x \equiv a_i \pmod{m_i}$, $i = 1, 2, ..., k$, where $k \geq 2$, $m_i \geq 2$ is an integer, $0 \leq a_i \leq m_i - 1$ is an integer, and $\gcd(m_i, m_j) = 1$ for all $1 \leq i < j \leq k$, can be obtained as follows.

   - Compute $M_i = m_1 \ldots m_{i-1} m_{i+1} \ldots m_k$ for all $1 \leq i \leq k$.
   - Find x_i satisfying $M_i x_i \equiv 1 \pmod{m_i}$ for all $1 \leq i \leq k$.
   - $x = a_1 M_1 x_1 + a_2 M_2 x_2 + \ldots + a_k M_k x_k$.

   Explain why the obtained x is a solution. (5%)
   Also find all solutions. (5%)

Sol: Notice that for $1 \leq r \leq k$, we have $a_r M_r x_r \equiv a_1 \pmod{m_1}$ if $r = 1$, and $a_r M_r x_r \equiv 0 \pmod{m_1}$ if $r \neq 1$. Hence,

$$a_1 M_1 x_1 + a_2 M_2 x_2 + \ldots + a_k M_k x_k \equiv a_1 \pmod{m_1}.$$

Similarly, $a_1 M_1 x_1 + a_2 M_2 x_2 + \ldots + a_k M_k x_k \equiv a_i \pmod{m_i}$ for $i = 2, 3, ..., k$.

Further, each $y \in [x]$ in Z_M, i.e., $y \equiv x \pmod{M}$, where $M = m_1 m_2 \ldots m_k$,
is also a solution.

10. Suppose that $(G, \cdot)$ is a group and $a \in G$. Prove that the inverse of a is unique. (10%)

Sol. Suppose that x and y are two inverses of a.
Then, $x = x \cdot e = x \cdot (a \cdot y) = (x \cdot a) \cdot y = e \cdot y = y$.

11. Explain why a cyclic group is abelian and why the group $(S_4, \cdot)$ is not cyclic, where S_4 is the set of 24 permutations on $\{1, 2, 3, 4\}$ (e.g., $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \in S_4$) and $\cdot$ denotes function composition (e.g., $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$). (10%)

Sol. Suppose that $(G, \cdot)$ is a cyclic group and a is a generator of G.
For any $x, y \in G$, we have $x = a^u$ and $y = a^v$ for some integers u and v.
Then, $x \cdot y = a^u \cdot a^v = a^{u+v} = a^{v+u} = a^v \cdot a^u = y \cdot x$, i.e., $(G, \cdot)$ is abelian.

On the other hand, since $(S_4, \cdot)$ is not abelian, e.g.,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

$(S_4, \cdot)$ is not a cyclic group.

12. Let G be a group with subgroups H and K. If $|G| = 330$, $|K| = 22$, and $K \subset H \subset G$, what are the possible values for $|H|$? (10%)

Sol: According to Lagrange's theorem, $|K|$ divides $|H|$, and $|H|$ divides $|G|$.
Since $22\ (= 2 \times 11) < |H| < 330\ (= 2 \times 3 \times 5 \times 11)$,
we have $|H| = 22 \times 3 = 66$ or $|H| = 22 \times 5 = 110$.