BÀI TẬP TUẦN 4

Bài 1. Cho tập $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$ là tập các thặng dư không âm nhỏ nhất theo modulo n. Với mọi $x, y \in \mathbb{Z}_n$, định nghĩa hai phép toán:

- $x * y = (x + y) \pmod n$,
- $x \circ y = xy \pmod n$ (x nhân y theo nghĩa phép nhân thông thường trên tập số nguyên).

Hãy chứng minh rằng $(\mathbb{Z}_n, *, \circ)$ là một vành

ta có: $\forall x, y \in \mathbb{Z}_n$

$$(x * y) = (x + y) \pmod n = (y + x) \pmod n = y * x$$

vậy $(\mathbb{Z}_n, *)$ có tính chất giao hoán

ta có: $\forall x, y, z \in \mathbb{Z}_n$

$$(x * y) * z = ((x + y) \pmod n) * z = ((x + y) \pmod n + z) \pmod n$$
$$= (x + (y + z) \pmod n) \pmod n = x * (y * z)$$

vậy $(\mathbb{Z}_n, *)$ có tính chất kết hợp

tồn tại $0 \in \mathbb{Z}_n$ là phần tử đơn vị vì

- $x * 0 = (x + 0) \pmod n = x$
- $0 * x = (0 + x) \pmod n = x$

với $\forall x \in \mathbb{Z}_n$ luôn tồn tại $x' = n - x$ thỏa:

$$x * x' = e \Leftrightarrow (x + (n - x)) \equiv 0 \pmod n$$

Vậy $(\mathbb{Z}_n, *)$ là 1 nhóm giao hoán

ta có: $\forall x, y, z \in \mathbb{Z}_n$

$$(x \circ y) \circ z = ((xy) \pmod n) \circ z = (xy \pmod n)z \pmod n$$
$$= x((yz) \pmod n) \pmod n = x \circ (y \circ z)$$

vậy phép toán $\circ$ của $\mathbb{Z}_n$ có tính chất kết hợp
ta có: $\forall x, y, z \in \mathbb{Z}_n$

$$x \circ (y * z) = x \circ ((y + z) \pmod n) = x(y + z) \pmod n$$
$$\Leftrightarrow xy + xz \pmod n$$

mà:

$$(y * z) \circ x = ((y + z) \pmod n)x \pmod n$$
$$= (y + z)x \pmod n = yx + zx \pmod n$$

Vậy phép toán $\circ$ có tính chất phân phối 2 bên với phép $*$
Từ những điều kiện thỏa mãn trên có thể nói rằng $(\mathbb{Z}_n, *, \circ)$

Bài 2. Chỉ ra rằng x là phần tử khả nghịch (có phần tử nghịch đảo) trên vành $(\mathbb{Z}_n, *, \circ)$ khi và chỉ khi x nguyên tố cùng nhau với n.

Để x khả nghịch trong $(\mathbb{Z}_n, *, \circ)$ tức là luôn tồn tại $y \in \mathbb{Z}_n$ sao cho

$$x \circ y = 1 \Leftrightarrow xy \equiv 1 \pmod n$$

Theo định lý Euler, luôn tồn tại $y \in \mathbb{Z}_n$ sao cho $\Leftrightarrow xy \equiv 1 \pmod n$ nếu $gcd(x, n) = 1$
do đó ra suy ra được nếu x là phần tử khả nghịch (có phần tử nghịch đảo) trên vành $(\mathbb{Z}_n, *, \circ)$ khi và chỉ khi x nguyên tố cùng nhau với n.

Bài 3. Gọi $\mathbb{Z}[x] = \{a_0 + a_x + a_2x + ... + a_nx^n : n \geq 0 \text{ và } a_0, a_1, ..., a_n \in \mathbb{Z}\}$ là tập các đa thức với hệ số là số nguyên. Chứng minh rằng $\mathbb{Z}[x]$ với phép cộng và phép nhân hai đa thức thông thường là một vành giao hoán có đơn vị

tồn tại $0 \in \mathbb{Z}[x]$ là phần tử đơn vị vì

- $f(x) + 0 = f(x)$
- $0 + f(x) = f(x)$

với $\forall f(x) \in \mathbb{Z}[x]$ luôn tồn tại $f'(x) = -f(x)$ thỏa:

$$f(x) + (-f'(x)) = 0$$

- Phép toán cộng và nhân của đa thức $\mathbb{Z}[x]$ có tính giao hoán và kết hợp vì $\mathbb{Z}$ là tập các số nguyên
- Phép Phân phối hai bên với phép cộng trong $\mathbb{Z}[x]$:

$$f(x).(g(x) + h(x)) = f(x).g(x) + f(x).h(x)$$

Tồn tại $1 \in \mathbb{Z}[x]$ là đơn vị nhân:

$$f(x).1 = f(x)$$

do đó: $(\mathbb{Z}[x], +)$ là nhóm giao hoán và cũng thỏa những tính chất của phép nhân trong đa thức.
Vậy $\mathbb{Z}[x]$ là một vành giao hoán có đơn vị.

Bài 4. Hãy chỉ ra rằng phương trình $x^2 + 14 = 0$ có bốn nghiệm trên vành $\mathbb{Z}_{15}$

phương trình:

$$x^2 + 14 \equiv 0 \pmod{15} \Leftrightarrow x^2 + 14 - 15 \equiv -15 \pmod{15} \Leftrightarrow x^2 - 1 \equiv 0 \pmod{15}$$

$$\Leftrightarrow (x-1)(x+1) \equiv 0 \pmod{15}$$

$\Rightarrow x \in \{1, 4, 11, \}$
vậy phương trình $x^2 + 14 = 0$ có bốn nghiệm trên vành $\mathbb{Z}_{15}$ là $x \in \{1, 4, 11, \}$

Bài 5. Hãy chứng tỏ rằng $(\mathbb{Z}_{17}, *, \circ)$ là một miền nguyên nhưng $(\mathbb{Z}_{16}, *, \circ)$ thì không phải là một miền nguyên.

Vành $(\mathbb{Z}_{17}, *, \circ)$ với 17 là số nguyên tố, nên với mọi $a, b \in \mathbb{Z}_{17} \setminus \{0\}, gcd(a, 17) = 1$.
suy ra $a \circ b = 0$ chỉ xảy ra khi $a = 0$ hoặc $b = 0$
Vậy $(\mathbb{Z}_{17}, *, \circ)$ là miền nguyên

Nhưng vành $(\mathbb{Z}_{16}, *, \circ)$ không phải là miền nguyên vì tồn tại $a = 4, b = 4$ với $(a, b \in \mathbb{Z}_{16}, a \neq 0, b \neq 0)$ thỏa:

$$a \circ b = 16 \pmod{16} = 0$$

do đó $(\mathbb{Z}_{16}, *, \circ)$ không phải là miền nguyên.

Bài 6. Cho p, q là các số nguyên tố. Hãy chứng minh rằng $(\mathbb{Z}_p, *, \circ)$ là một miền nguyên nhưng $(\mathbb{Z}_{pq}, *, \circ)$ thì không phải là một miền nguyên

với p là số nguyên tố. Trong $\mathbb{Z}_p$ mọi phần tử $x \neq 0$ đều có $gcd(x, p) = 1$
nên $x \circ y = (xy) \pmod{p} \neq 0$ khi và chỉ khi $x \neq 0$ và $y \neq 0$
Vì không tồn tại $x, y \neq 0$ mà $x \circ y = 0$
Vậy $(\mathbb{Z}_p, *, \circ)$ là miền nguyên.

Nhưng vành $(\mathbb{Z}_{pq}, *, \circ)$ không phải miền nguyên vì:
tồn tại $x = p, y = q$ với $(x, y \in \mathbb{Z}_{16}, x \neq 0, y \neq 0)$ thỏa:

$$x \circ y = (pq) \pmod{pq} = 0$$

do đó $(\mathbb{Z}_{pq}, *, \circ)$ không phải là miền nguyên.

Bài 7. Chứng minh rằng $(\mathbb{Z}_n, *, \circ)$ với các phép toán được định nghĩa như ở Bài 1 là một trường khi và chỉ khi n là số nguyên tố.

Vì n là số nguyên tố, thì $(\mathbb{Z}_n, *, \circ)$ là vành:
ta có: n là số nguyên tố, thì $\forall x \in \mathbb{Z}_n, x \neq 0$ đều thỏa $gcd(x, n) = 1$
Điều này đảm bảo: $x \circ y = 1$ luôn có nghiệm y. (định lý euler)
Do đó: $(\mathbb{Z}_n, *, \circ)$ là một trường khi n là số nguyên tố

Nếu n không phải là số nguyên tố thì sẽ tồn tại $d > 1$ sao cho $d|n$ với $x = d$ ta có $gcd(x, n) > 1$. khi đó, phương trình $x \circ y = 1$ không có nghiệm $y \in \mathbb{Z}_n$.

Vậy $(\mathbb{Z}_n, *, \circ)$ là một trường khi n là số nguyên tố.