

NGUYỄN GIA ĐÌNH - VŨ VĂN TUẤN DÙNG

BÀI TẬP

BÀI TẬP SỐ ĐẠI CHƯƠNG

PGS.TS. NGUYỄN GIA ĐỊNH - TS. VÕ VĂN TUẤN DŨNG

BÀI TẬP ĐẠI SỐ ĐẠI CƯƠNG

MỤC LỤC

Bài tập Chương I – Nhóm	5
Trả lời và hướng dẫn giải bài tập Chương I – Nhóm	12
Bài tập Chương II – Vành	30
Trả lời và hướng dẫn giải bài tập Chương II – Vành	36
Bài tập Chương III – Vành đa thức	55
Trả lời và hướng dẫn giải bài tập Chương III – Vành đa thức	59
Bài tập Chương IV – Môđun	69
Trả lời và hướng dẫn giải bài tập Chương IV – Môđun	76
Tài liệu tham khảo	90

BÀI TẬP CHƯƠNG I – NHÓM

1. Trên tập hợp \mathbb{Q} các số hữu tỉ, xét phép toán $*$ xác định như sau:

$$\forall a, b \in \mathbb{Q}, \quad a * b = a + b + ab.$$

a) \mathbb{Q} cùng phép toán $*$ có phải là một nhóm không? Tại sao?

b) Chứng minh $\mathbb{Q} \setminus \{-1\}$ cùng phép toán $*$ tạo thành một nhóm.

2. Chứng minh tập hợp $G = \{(a, b) \mid a, b \in \mathbb{R}, b \neq 0\}$ cùng phép toán ký hiệu nhân

$$\forall (a, b), (a', b') \in G, \quad (a, b)(a', b') = (ab' + a', bb')$$

là một nhóm và $H = \{(a, 1) \mid a \in \mathbb{R}\}$ là một nhóm con của G .

3. Cho $G = \mathbb{R}^* \times \mathbb{R}$ (với \mathbb{R} là tập hợp các số thực và $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$) và là phép toán trên G xác định bởi:

$$(x, y) * (x', y') = (xx', xy' + \frac{y}{x'}).$$

a) Chứng minh rằng $(G, *)$ là một nhóm.

b) Chứng tỏ rằng với bất kỳ $k \in \mathbb{R}$, tập hợp $H_k = \{(x, k(x - \frac{1}{x})) \mid x \in \mathbb{R}^*\}$ là một nhóm con giao hoán của G .

c) Hãy xác định tâm $Z(G)$ của G .

4. Trên tập hợp $G = [0, 1) = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$, xét phép toán \oplus như sau:

$$\forall x, y \in G, \quad x \oplus y = x + y - [x + y]$$

(ở đây $[x + y]$ là phần nguyên của $x + y$).

a) Chứng minh (G, \oplus) là một nhóm abel.

b) Chứng minh rằng ánh xạ $f : G \longrightarrow \mathbb{C}^*$ xác định bởi $f(x) = \cos 2\pi x + i \sin 2\pi x$, là một đồng cấu nhóm, trong đó \mathbb{C}^* là nhóm nhân các số phức khác 0.

5. Chứng minh rằng một nhóm mà không có nhóm con thực sự là nhóm đơn vi hoặc là nhóm cyclic có cấp nguyên tố.

6. Cho G là một nhóm và H là một nhóm con chuẩn tắc của G sao cho $H \subset Z(G)$. Chứng minh rằng nếu G/H là một nhóm cyclic thì G là nhóm abel.

7. Cho G là một nhóm nhán và H là một nhóm con của G . Chứng minh:

- a) Nếu $[G : H] = 2$ thì $H \triangleleft G$.
- b) Nếu $H \triangleleft G$ và $[G : H] = m$ thì $a^m \in H, \forall a \in G$.

8. Cho G là một nhóm nhán, A và B là hai nhóm con của G . Ký hiệu:

$$AB = \{ab \mid a \in A \text{ và } b \in B\}, BA = \{ba \mid b \in B \text{ và } a \in A\}$$

Chứng minh rằng AB là một nhóm con của G khi và chỉ khi $AB = BA$.

9. Cho G là một nhóm, A, B, C là các nhóm con của G . Chứng minh:

- a) $A \cap B$ là một nhóm con của G .
- b) $A \cup B$ là nhóm con của G khi và chỉ khi $A \subset B$ hoặc $B \subset A$.
- c) Nếu $C \subset A \cup B$ thì $C \subset A$ hoặc $C \subset B$.

10. Cho G là một nhóm nhán có tính chất: $\forall x \in G, x^2 = 1$, với 1 là phần tử trung hoà của nhóm G . Chứng tỏ rằng:

- a) G là một nhóm aben.
- b) Nếu G là nhóm hữu hạn thì tồn tại số tự nhiên n sao cho số phần tử của nhóm G bằng 2^n .

11. Cho G là một nhóm và A, B, C, K là các nhóm con của G . Chứng minh rằng:

- a) Nếu $A \subset C$ thì $AB \cap C = A(B \cap C)$. (Lưu ý rằng AB không nhất thiết là một nhóm con của G .)
- b) Nếu $A \subset B, A \cap K = B \cap K$ và $AK = BK$ thì $A = B$.

12. a) Xét trường \mathbb{Z}_{13} các số nguyên modulo 13. Hãy lập bảng nhân của \mathbb{Z}_{13}^* . Chứng tỏ rằng $\mathbb{Z}_{13}^* = \mathbb{Z}_{13} \setminus \{0\}$ là một nhóm nhán cyclic.

b) Xét trường \mathbb{R} các số thực. Khi đó $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ có phải là một nhóm nhán cyclic không?

13. Trong nhóm nhán \mathbb{C}^* các số phức khác không, hãy xác định nhóm con cyclic sinh bởi phần tử $x \in \mathbb{C}^*$, trong đó

$$a) x = -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i,$$

$$b) x = \cos \frac{4\pi}{7} + i \sin \frac{4\pi}{7}.$$

14. Cho S_3 là tập hợp tất cả các hoán vị của tập hợp $\{1, 2, 3\}$.

- a) Hãy lập bảng nhân của S_3 , chứng tỏ S_3 là một nhóm.

b) Tìm tất cả các nhóm con chuẩn tắc của S_3 .

c) Cho G_1 và G_2 là hai nhóm có cấp lần lượt là 24 và 30. Hãy mô tả nhóm không giao hoán G_3 là ánh đồng cấu của cả G_1 và G_2 (qua phép đồng cấu).

15. Xét nhóm \mathbb{Q} các số hữu tỉ với phép cộng thông thường. Chứng minh rằng:

a) \mathbb{Q} không là nhóm cyclic;

b) \mathbb{Q}/\mathbb{Z} có đồng cấu với \mathbb{Q} không?

16. Ký hiệu $H = \left\{ \begin{pmatrix} m & b \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}_7) \mid m, b \in \mathbb{Z}_7, m = \pm 1 \right\}$,

trong đó $\mathrm{GL}(2, \mathbb{Z}_7)$ là nhóm nhân các ma trận vuông cấp 2 khả nghịch lấy hệ số trên trường \mathbb{Z}_7 các số nguyên modulo 7. Chứng minh rằng:

a) H là nhóm con của nhóm $\mathrm{GL}(2, \mathbb{Z}_7)$ có 14 phần tử.

b) Mọi phần tử của H có thể viết được duy nhất dưới dạng $A^i B^j$, trong đó $0 \leq i < 7$, $0 \leq j < 2$ và $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.

17. Cho G là nhóm nhân được sinh bởi hai phần tử x và y với các quan hệ:

$$x^3 = y^2 = (xy)^2 = 1.$$

a) Xác định các phần tử của nhóm G và lập bảng nhân của G .

b) Tìm tất cả các nhóm con của nhóm G .

18. Cho G là nhóm với phép nhân ma trận, được sinh bởi hai ma trận hệ số thực $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ và $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

a) Xác định các phần tử của nhóm G .

b) Tìm tất cả các nhóm con của G .

19. Cho G là một nhóm nhân và n là một số nguyên dương sao cho

$$f_n : G \longrightarrow G : x \mapsto x^n$$

là một toàn cấu nhóm. Chứng minh rằng:

a) $x^{n-1}y = yx^{n-1}$, $\forall x, y \in G$.

b) Với $n = 3$, G là một nhóm aben.

MATH-EDUCARE

20. Cho G là một nhóm sao cho có một số nguyên $n > 1$ thoả mãn $(xy)^n = x^n y^n$, $\forall x, y \in G$. Ký hiệu:

$$G^{(n)} = \{x^n \mid x \in G\}, \quad G_{(n)} = \{x \in G \mid x^n = 1\}.$$

Chứng minh rằng:

- a) $G^{(n)} \triangleleft G$ và $G_{(n)} \triangleleft G$.
- b) $G/G_{(n)} \cong G^{(n)}$.

21. a) Cho H là nhóm con của nhóm nhân $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ gồm các số phức có môđun bằng 1, \mathbb{R}_+^* là nhóm nhân gồm các số thực dương. Chứng minh rằng \mathbb{C}^*/H đẳng cấu với \mathbb{R}_+^* .

b) Cho $f : G \longrightarrow H$ là một toàn cầu nhóm, M là một nhóm con chuẩn tắc của H , $N = f^{-1}(M)$. Chứng minh rằng N là nhóm con chuẩn tắc của G và G/N đẳng cấu với H/M .

22. Chứng minh rằng:

- a) Nếu G là nhóm cyclic thì $\text{Aut}(G)$ là nhóm aben.
- b) Nếu G là nhóm cyclic cấp p nguyên tố thì $\text{Aut}(G)$ là cyclic cấp $p - 1$.

23. Cho $f : G \longrightarrow K$ là một đồng cấu nhóm. Chứng minh rằng:

- a) Nếu cấp của G là hữu hạn thì cấp của $f(G)$ chia hết cấp của G .
- b) Nếu H là nhóm con có chỉ số n trong G , $\text{Ker } f \subset H$ và f là toàn cầu thì $f(H)$ có chỉ số n trong K .

24. Cho G là một nhóm, $C_g : G \longrightarrow G$ là ánh xạ với $g \in G$ xác định bởi $C_g(x) = gxg^{-1}$. Ký hiệu:

$$\text{Aut}(G) = \{f : G \longrightarrow G \mid f \text{ là đẳng cấu}\}, \quad \text{Inn}(G) = \{C_g \mid g \in G\}.$$

Chứng tỏ rằng:

- a) C_g là một tự đẳng cấu, $\text{Aut}(G)$ là một nhóm với phép toán hợp thành và $\text{Inn}(G)$ là một nhóm con chuẩn tắc của $\text{Aut}(G)$.
- b) $Z(G) = \{a \in G \mid ax = xa, \forall x \in G\}$ là một nhóm con chuẩn tắc của G (gọi là tâm của nhóm G) và $G/Z(G) \cong \text{Inn}(G)$.

25. Cho G là một nhóm, với $x, y \in G$, ký hiệu $[x, y] = x^{-1}y^{-1}xy$ (gọi là giao hoán tử của x và y). Gọi $[G, G]$ là nhóm con của G sinh ra bởi tập $\{[x, y] \mid x, y \in G\}$. Chứng minh rằng:

a) $[G, G]$ là nhóm con chuẩn tắc nhỏ nhất của G sao cho $G/[G, G]$ là aben.

b) $[xy, z] = y^{-1}[x, z]y[y, z], \forall x, y, z \in G;$

c) Nếu $[G, G] \subset Z(G)$ (tâm của G) thì với $a \in G$, ánh xạ $f : G \rightarrow G$ xác định bởi $f(x) = [x, a]$ là một đồng cấu. Tìm $\text{Ker}(f)$.

d) Hãy xác định $[S_3, S_3]$, trong đó S_3 là nhóm các hoán vị của 3 số 1, 2, 3 và chứng minh $S_3/S'_3 \cong \mathbb{Z}_2$.

26. Cho G là một nhóm, $a \in G$ là phần tử có cấp hữu hạn n . Chứng minh rằng với mọi số nguyên dương m , cấp của phần tử a^m là

$$\text{ord } (a^m) = \frac{n}{(m, n)},$$

trong đó (m, n) là ước chung lớn nhất của m và n .

27. a) Cho $G = \langle g \rangle$ là nhóm cyclic cấp 168. Tìm cấp của phần tử g^{132} .

b) Tìm tất cả các phần tử cấp 14 của nhóm cộng \mathbb{Z}_{140} các số nguyên modulo 140.

28. Cho C là một nhóm cyclic sinh bởi phần tử a . Chứng minh rằng:

a) Nếu G là một nhóm con của C thì G cũng là một nhóm cyclic.

b) Nếu C là nhóm hữu hạn và m là số nguyên dương ước của $|C|$ thì tồn tại duy nhất nhóm con G của C sao cho $|G| = m$.

c) Nếu C là nhóm vô hạn thì C có 2 phần tử sinh là a và a^{-1} .

d) Nếu $|C| = n$ thì a^n là phần tử sinh của C khi và chỉ khi n và n nguyên tố cùng nhau.

29. Xét nhóm cộng \mathbb{Q} các số hữu tỉ. Chứng minh rằng ánh xạ $f : \mathbb{Q} \rightarrow \mathbb{Q}$ là đồng cấu nhóm khi và chỉ khi tồn tại duy nhất một số $a \in \mathbb{Q}$ sao cho $f(x) = ax, \forall x \in \mathbb{Q}$.

30. Xét nhóm cộng \mathbb{Q} các số hữu tỉ và nhóm nhân \mathbb{Q}^+ các số hữu tỉ dương. Hãy tìm các đồng cấu nhóm $f : \mathbb{Q} \rightarrow \mathbb{Q}^+$.

31. Cho G là một nhóm có cấp $2n$, với n là một số tự nhiên lẻ và H là một nhóm con cấp n của G thoả mãn:

$$xhx^{-1} = h^{-1}, \forall x \in G \setminus H, \forall h \in H.$$

(Ở đây, $G \setminus H$ là phần bù của H trong G .) Chứng minh rằng H là một nhóm aben và mọi phần tử của $G \setminus H$ đều có cấp 2.

32. Cho m và n là hai số nguyên dương nguyên tố cùng nhau. Chứng minh rằng đẳng cấu nhóm $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$. Từ đó suy ra $\mathbb{Z}_3 \times \mathbb{Z}_2$ không đẳng cấu với nhóm đối xứng S_3 .

33. Cho G là một nhóm, M và N là hai nhóm con chuẩn tắc của G sao cho $G = MN$. Chứng minh rằng

$$G/(M \cap N) \cong G/M \times G/N.$$

34. a) Trên tập hợp $G = \mathbb{Z}^3$, với \mathbb{Z} là tập các số nguyên, xét phép toán hai ngôi:

$$\forall (a, b, c), (a', b', c') \in G, (a, b, c) * (a', b', c') = (a + a', b + b', c + c' - ba').$$

Chứng minh rằng $(G, *)$ là một nhóm không aben.

b) Trên tập hợp \mathbb{R}^2 các cặp số thực, xét phép toán \circ :

$$(x, y) \circ (x', y') = (xx' - yy', yx' + xy').$$

(\mathbb{R}^2, \circ) có là một nhóm không?

35. Xét nhóm \mathbb{R} các số thực với phép toán hai ngôi:

$$\forall x, y \in \mathbb{R}, x * y = x\sqrt{1+y^2} + y\sqrt{1+x^2}$$

và ánh xạ $f : \mathbb{R} \rightarrow \mathbb{R}$ xác định bởi $f(x) = \frac{e^x - e^{-x}}{2}$. Chứng minh rằng f là một đẳng cấu từ nhóm $(\mathbb{R}, +)$ lên nhóm $(\mathbb{R}, *)$.

36. Ký hiệu U_n là nhóm nhân các phần tử khả nghịch của vành \mathbb{Z}_n các số nguyên môđulô n .

a) Lập bảng nhân của U_{22} và chứng minh rằng U_{22} là một nhóm cyclic.

b) U_{24} có là nhóm cyclic không? Vì sao?

37. Cho R là một vành có đơn vị 1. Trên R , xét phép toán $*$:

$$x * y = x + y - xy.$$

Ký hiệu $R_* = \{x \in R \mid \exists y \in R, x * y = y * x = 0\}$. Chứng minh rằng:

a) $(R_*, *)$ là một nhóm.

b) $R_* \cong U(R)$, với $U(R)$ là nhóm các phần tử khả nghịch của vành R .

38. Cho G là một nhóm nhàn hữu hạn sao cho G có một tự đẳng cấu φ thoả mãn $\varphi(a) \neq a$, $\forall a \neq 1_G$. Chứng minh rằng:

a) Với mọi $\alpha \in G$, tồn tại $g \in G$ sao cho $\alpha = g^{-1}\varphi(g)$.

b) Nếu φ có cấp bằng 2, tức là $\varphi \neq id$ và $\varphi^2 = id$ thì $\varphi(\alpha) = \alpha^{-1}$ với mọi $\alpha \in G$ và G là một nhóm aben có cấp là một số lẻ.

39. Đặt G là tập hợp các ma trận vuông cấp 2 hệ số thực có dạng

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \quad (a, b \in \mathbb{R}, a \neq 0)$$

và $H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{R} \right\}$. Chứng minh rằng:

a) G là một nhóm với phép nhân ma trận và H là nhóm con chuẩn tắc của G .

b) Nhóm thương G/H đẳng cấu với nhóm nhân \mathbb{R}^* các số thực khác không.

40. Đặt P là tập hợp các ma trận vuông cấp 3, tam giác trên, khá nghịch có hệ số thực.

a) Chứng minh rằng P là một nhóm không giao hoán với phép nhân ma trận.

b) Tìm các phần tử của P có cấp 2.

41. Xét nhóm thay phiên A_4 (nhóm con của nhóm đối xứng S_4 gồm các phép thay chẵn bậc 4).

a) Chứng tỏ rằng nhóm A_4 không có nhóm con cấp 6.

b) Tìm tất cả các p -nhóm con Sylow của A_4 với $p = 2$ và 3.

42. Cho G là một nhóm hữu hạn có cấp là $p^r m$, với $r \geq 1$ và $p \nmid m$. Chứng minh rằng:

a) Nếu P là một p -nhóm con Sylow của G và H là một p -nhóm sao cho $P \subset H \subset G$ thì $H = P$.

b) Nếu G chỉ có p -nhóm con Sylow duy nhất là P thì $P \trianglelefteq G$.

43. Cho G là một nhóm hữu hạn có cấp là pq , trong đó p và q là hai số nguyên tố mà $p < q$. Chứng minh rằng:

a) G có một và chỉ một nhóm con cấp q .

b) Nếu $q \neq 1 + kp$ với số nguyên k tùy ý thì G là nhóm cyclic cấp

TRẢ LỜI VÀ HƯỚNG DẪN GIẢI BÀI TẬP

CHƯƠNG I – NHÓM

1. $\forall a, b, c \in \mathbb{Q}$, $(a * b) * c = (a + b + ab) * c = a + b + ab + c + ac + bc + abc = a + b + c + bc + ab + ac + abc = a * (b + c + bc) = a * (b * c)$, hay phép toán $*$ có tính kết hợp. $\forall a \in \mathbb{Q}$, $a * 0 = 0 * a = a$ hay 0 là phần tử đơn vị của \mathbb{Q} đối với phép toán $*$. Do đó \mathbb{Q} với phép toán $*$ là một vị nhóm, nhưng không phải là một nhóm, vì phần tử $a = -1$ không có phần tử nghịch đảo.

Từ $a + b + ab + 1 = (a+1)(b+1)$, ta có $\forall a, b \in \mathbb{Q} \setminus \{-1\}$, $a * b \neq -1$ hay $a * b \in \mathbb{Q} \setminus \{-1\}$. Do đó $\mathbb{Q} \setminus \{-1\}$ là một vị nhóm với phép toán $*$. Ngoài ra, $\forall a \in \mathbb{Q} \setminus \{-1\}$, a có phần tử nghịch đảo là $-\frac{a}{1+a} \in \mathbb{Q} \setminus \{-1\}$. Vậy $\mathbb{Q} \setminus \{-1\}$ là một nhóm với phép toán $*$.

2. $\forall (a, b), (a', b'), (a'', b'') \in G$,

$((a, b)(a', b'))(a'', b'') = (ab' + a', bb')(a'', b'') = (ab'b'' + a'b'' + a'', bb'b'') = (a, b)(a'b'' + a'', b'b'') = (a, b)((a', b')(a'', b''))$ hay phép toán nhân có tính kết hợp. $\forall (a, b) \in G$, $(a, b)(0, 1) = (0, 1)(a, b) = (a, b)$ hay $(0, 1)$ là phần tử đơn vị của G . $\forall (a, b) \in G$, $(a, b)(-\frac{a}{b}, \frac{1}{b}) = (-\frac{a}{b}, \frac{1}{b})(a, b) = (0, 1)$ hay (a, b) có phần tử nghịch đảo là $(-\frac{a}{b}, \frac{1}{b})$. Vậy G là một nhóm.

$H \neq \emptyset$ vì $(0, 1) \in H$. $\forall (a, 1), (a', 1) \in H$, $(a, 1)(a', 1)^{-1} = (a, 1)(-\frac{a'}{1}, \frac{1}{1}) = (a - a', 1) \in H$. Vậy H là một nhóm con của G .

3. a) $\forall (x, y), (x', y'), (x'', y'') \in G$,

$$\begin{aligned} ((x, y) * (x', y')) * (x'', y'') &= (xx', xy' + \frac{y}{x'}) * (x'', y'') = (xx'x'', xx'y'' + \frac{xy'}{x''} + \frac{y}{x'x''}) \\ &= (x(x'x''), x(x'y'' + \frac{y'}{x''}) + \frac{y}{x'x''}) = (x, y) * (x'x'', x'y'' + \frac{y'}{x''}) = (x, y) * ((x', y') * (x'', y'')). \end{aligned}$$

$$\forall (x, y) \in G, (x, y) * (1, 0) = (x, y) = (0, 1) * (x, y).$$

$$\forall (x, y) \in G, (x, y) * (\frac{1}{x}, -y) = (1, 0) = (\frac{1}{x}, -y) * (x, y).$$

Vậy G là một nhóm.

b) $(1, 0) = (1, k(1 - \frac{1}{1})) \in H_k$ nên $H_k \neq \emptyset$.

$$\forall (x, k(x - \frac{1}{x})), (y, k(y - \frac{1}{y})) \in H_k,$$

$$(x, k(x - \frac{1}{x})) * (y, k(y - \frac{1}{y}))^{-1} = (x, k(x - \frac{1}{x})) * (\frac{1}{y}, k(\frac{1}{y} - y)) = \\ (\frac{x}{y}, k(\frac{x}{y} - \frac{y}{x})) \in H_k.$$

$$(x, k(x - \frac{1}{x})) * (y, k(y - \frac{1}{y})) = (xy, k(xy - \frac{1}{xy})) = (y, k(y - \frac{1}{y})) * \\ (x, k(x - \frac{1}{x})).$$

Vậy H_k là một nhóm con giao hoán của G .

$$\begin{aligned} Z(G) &= \{(x, y) \mid (x, y) * (a, b) = (a, b) * (x, y), \forall (a, b) \in G\} \\ &= \{(x, y) \mid (xa, xb + \frac{y}{a}) = (ax, ay + \frac{b}{x}), \forall (a, b) \in G\} \\ &= \{(x, y) \mid b(x - \frac{1}{x}) = y(a - \frac{1}{a}), \forall (a, b) \in G\} \\ &= \{(x, y) \mid x - \frac{1}{x} = 0, y = 0\} \\ &= \{(1, 0), (-1, 0)\}. \end{aligned}$$

4. Trước hết ta có $\forall x \in \mathbb{R}, \forall n \in \mathbb{Z}, [x + n] = [x] + n$.

$$\forall x, y \in G, (x \oplus y) = x + y - [x + y] = y + x - [y + x] = y \oplus x.$$

$$\begin{aligned} \forall x, y, z \in G, (x \oplus y) \oplus z &= x \oplus y + z - [x \oplus y + z] = x + y - [x + y] + z - [x + y + z - [x + y]] \\ &= x + y + z - [x + y + z - [x + y]] = x + y + z - [x + y] - [x + y + z] + [x + y] = \\ &= x + y + z - [x + y + z] = x + y + z - [y + z] - [x + y + z] + [y + z] = \\ &= x + y + z - [y + z] - [x + y + z - [y + z]] = x + y \oplus z - [x + y \oplus z] = x \oplus (y \oplus z). \end{aligned}$$

$$\forall x \in G, [x] = 0 \text{ nên } x \oplus 0 = x + 0 - [x + 0] = x.$$

$\forall x \in G$, nếu $x = 0$ thì $0 \oplus 0 = 0$, nếu $x \neq 0$ thì $1 - x \in G$ và $x \oplus (1 - x) = 0$.

Vậy (G, \oplus) là một nhóm aben.

$$\text{b)} \forall x, y \in G, f(x \oplus y) = \cos 2\pi(x \oplus y) + i \sin 2\pi(x \oplus y) = \cos(2\pi x + 2\pi y - 2\pi[x + y]) + i \sin(2\pi x + 2\pi y - 2\pi[x + y]) = \cos(2\pi x + 2\pi y) + i \sin(2\pi x + 2\pi y) = (\cos 2\pi x + i \sin 2\pi x)(\cos 2\pi y + i \sin 2\pi y) = f(x)f(y).$$

Vậy f là một đồng cấu nhóm.

5. Giả sử G là một nhóm mà không có nhóm con thực sự nào. Nếu $G \neq \{1\}$ thì tồn tại $a \in G$ với $a \neq 1$. Nhóm con $\langle a \rangle$ của G sinh ra bởi a khác $\{1\}$ nên phải bằng G hay G là nhóm cyclic. Nếu G có cấp p và giả sử $p = mn$ với $1 < m, n < p$ thì G có nhóm con cấp m , đây là nhóm con thực sự của G . Điều này dẫn đến p là số nguyên tố.

6. Giả sử $G/H = \langle aH \rangle$ ($a \in G$). $\forall x, y \in G, \exists m, n \in \mathbb{Z}$ sao cho $xH = (aH)^m = a^mH, yH = (aH)^n = a^nH$. Khi đó $x = \underline{a^m u}$ và $y = \underline{a^n v}$, với $u, v \in H$ (nên thuộc $Z(G)$).

$$xy = a^m u a^n v = a^m a^n u v = a^{m+n} v u = a^n a^m v u = a^n v a^m u = yx.$$

Vậy G là một nhóm aben.

7. a) G có đúng hai lớp kề là xH và H , trong đó $x \notin H$. Khi đó, với mọi $g \in G = H \cup xH$, với mọi $a \in H$, ta có $gag^{-1} \in H$ khi $g \in H$ và khi $g \notin H$ nghĩa là $g = xh$ với $h \in H$ thì $gag^{-1} = xhah^{-1}x^{-1} \in H$, vì nếu ngược lại $xhah^{-1}x^{-1} = xh'$ với $h' \in H$ hay $x = h'^{-1}hah^{-1} \in H$, điều này vô lý. Do đó $H \triangleleft G$.

b) Do $H \triangleleft G$ nên ta có nhóm thương G/H có cấp là $|G/H| = [G : H] = m$. Do đó với mọi $a \in G$, $aH \in G/H$, ta có $a^mH = (aH)^m = H$ hay $a^m \in H$.

8.

- $AB \leq G$:

$x \in AB \Rightarrow x^{-1} \in AB$ (vì $AB \leq G$) $\Rightarrow x^{-1} = ab$, $a \in A$, $b \in B \Rightarrow x = b^{-1}a^{-1} \in BA$ (vì $b^{-1} \in B$ và $a^{-1} \in A$). Do đó $AB \subset BA$.

$x \in BA \Rightarrow x = ba$, $b \in B$, $a \in A \Rightarrow x^{-1} = a^{-1}b^{-1} \in AB$ (vì $a^{-1} \in A$ và $b^{-1} \in B$) $\Rightarrow x \in AB$ (vì $AB \leq G$). Do đó $BA \subset AB$.

Vậy $AB = BA$.

- $AB = BA$:

$$1 = 1 \cdot 1 \in AB \Rightarrow AB \neq \emptyset.$$

$x, x_1 \in AB \Rightarrow x = ab$, $x_1 = a_1b_1$, $a, a_1 \in A$, $b, b_1 \in B \Rightarrow xx_1^{-1} = abb_1^{-1}a_1^{-1}$.

$b' = bb_1^{-1} \in B \Rightarrow b'a_1^{-1} \in BA = AB \Rightarrow b'a_1^{-1} = a_2b_2$, $a_2 \in A$, $b_2 \in B \Rightarrow xx_1^{-1} = ab'a_1^{-1} = aa_2b_2 \in AB$ (vì $aa_2 \in A$ và $b_2 \in B$).

Vậy AB là một nhóm con của G .

9. a) Ký hiệu 1 là đơn vị của G .

$$1 \in A \wedge 1 \in B \Rightarrow 1 \in A \cap B \Rightarrow A \cap B \neq \emptyset.$$

$\forall x, y \in A \cap B \Rightarrow x, y \in A \wedge x, y \in B \Rightarrow xy^{-1} \in A \wedge xy^{-1} \in B \Rightarrow xy^{-1} \in A \cap B$.

Vậy $A \cap B$ là một nhóm con của G .

b) Giả sử $A \cup B$ là một nhóm con của G và $A \not\subset B$. Khi đó $\exists a \in A$, $a \notin B$ và $\forall b \in B$, $c = ab \in A \cup B$ (vì $A \cup B$ là một nhóm con của G) hay $c \in A$ hoặc $c \in B$. Nếu $c \in B$ thì $a = cb^{-1} \in B$, mâu thuẫn với $a \notin B$. Vậy $c \in A$, suy ra $b = a^{-1}c \in A$. Do đó $B \subset A$.

Ngược lại, nếu $A \subset B$ thì $A \cup B = B$ là một nhóm con của G và nếu $B \subset A$ thì $A \cup B = A$ là một nhóm con của G .

c) Giả sử $C \subset A \cup B$ và $C \not\subset A$. Khi đó $\exists c_0 \in C$, $c_0 \notin A$ nên $c_0 \in B$ (vì $c_0 \in A \cup B$).

$\forall c \in C (\Rightarrow c \in A \cup B \Rightarrow c \in A \vee c \in B) \Rightarrow b = cc_0 \in C \Rightarrow b \in A \vee b \in B$.

- Với $c \in A$, nếu $b \in A$ thì $c_0 = c^{-1}b \in A$, mâu thuẫn với $c_0 \notin A$.
Vậy $b \in B$, nên $c = bc_0^{-1} \in B$.

- Với $c \in B$ thì bài toán được chứng minh; tức là, $C \subset B$.

10. a) $\forall x, y \in G, x^2y^2 = (xy)^2 (= 1)$ hay $xxyy = xyxy$, do đó $xy = yx$. Vậy G là một nhóm aben.

b) Xem phép toán trên G là phép cộng, khi đó ta có $2x = 0, \forall x \in G$. Vì vậy có phép nhân vô hướng của \mathbb{Z}_2 lên G :

$$\forall \bar{a} \in \mathbb{Z}_2, \forall x \in G, \bar{a}x = ax.$$

Kiểm chứng dễ dàng G là một \mathbb{Z}_2 -không gian vectơ, do G hữu hạn nên G là không gian vectơ hữu hạn chiều. Giả sử $\dim G = n$. Khi đó $G \cong \mathbb{Z}_2^n$ hay $|G| = 2^n$.

11. a) Cho $ac \in A(B \cap C)$, trong đó $a \in A$ và $c \in B \cap C$. Khi đó $ac \in AB$ và $ac \in aC = C$. Vì thế $A(B \cap C) \subset AB \cap C$. Mặt khác, nếu $ab \in AB \cap C$, trong đó $a \in A$ và $b \in B$ thì $b \in a^{-1}C = C$ và vì vậy $ab \in A(B \cap C)$. Vậy $AB \cap C \subset A(B \cap C)$.

b) Theo a) và các giả thiết, ta có

$$A = A(A \cap K) = A(B \cap K) = AK \cap B = BK \cap B = B.$$

12. a) Bảng nhân của \mathbb{Z}_{13} :

.	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12
2	0	2	4	6	8	10	12	1	3	5	7	9	11
3	0	3	6	9	12	2	5	8	11	1	4	7	10
4	0	4	8	12	3	7	11	2	6	10	1	5	9
5	0	5	10	2	7	12	4	9	1	6	11	3	8
6	0	6	12	5	11	4	10	3	9	2	8	1	7
7	0	7	1	8	2	9	3	10	4	11	5	12	6
8	0	8	3	11	6	1	9	4	12	7	2	10	5
9	0	9	5	1	10	6	2	11	7	3	12	8	4
10	0	10	7	4	1	11	8	5	2	12	9	6	3
11	0	11	9	7	5	3	1	12	10	8	6	4	2
12	0	12	11	10	9	8	7	6	5	4	3	2	1

$$\begin{aligned}\bar{2}^1 &= \bar{2}, \bar{2}^2 = \bar{4}, \bar{2}^3 = \bar{8}, \bar{2}^4 = \bar{3}, \bar{2}^5 = \bar{6}, \bar{2}^6 = \bar{12}, \\ \bar{2}^7 &= \bar{11}, \bar{2}^8 = \bar{9}, \bar{2}^9 = \bar{5}, \bar{2}^{10} = \bar{10}, \bar{2}^{11} = \bar{7}, \bar{2}^{12} = \bar{1}.\end{aligned}$$

Như vậy, \mathbb{Z}_{13}^* là một nhóm cyclic với phần tử sinh là $\bar{2}$.

b) Giả sử \mathbb{R}^* là một nhóm cyclic sinh bởi x , nghĩa là

$$\mathbb{R}^* = \{x^n \mid n \in \mathbb{Z}\}.$$

Khi đó ánh xạ $f : \mathbb{Z} \rightarrow \mathbb{R}^*$ cho bởi $f(n) = x^n$ là một toàn ánh, nên \mathbb{R}^* là không quá đếm được. Điều này vô lý vì \mathbb{R}^* là tập hợp vô hạn không đếm được. Vậy \mathbb{R}^* không là nhóm cyclic.

13. a)

$$\begin{aligned}x &= -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i, x^2 = -i, x^3 = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i, x^4 = -1, \\ x^5 &= \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i, x^6 = i, x^7 = -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i, x^8 = 1.\end{aligned}$$

$$\text{Vậy } \langle x \rangle = \{1, x, x^2, x^3, x^4, x^5, x^6, x^7\}.$$

b)

$$\begin{aligned}x &= \cos \frac{4\pi}{7} + i \sin \frac{4\pi}{7}, x^2 = \cos \frac{8\pi}{7} + i \sin \frac{8\pi}{7}, \\ x^3 &= \cos \frac{12\pi}{7} + i \sin \frac{12\pi}{7}, x^4 = \cos \frac{2\pi}{7} + i \sin \frac{2\pi}{7}, \\ x^5 &= \cos \frac{6\pi}{7} + i \sin \frac{6\pi}{7}, x^6 = \cos \frac{10\pi}{7} + i \sin \frac{10\pi}{7}, x^7 = 1.\end{aligned}$$

$$\text{Vậy } \langle x \rangle = \{1, x, x^2, x^3, x^4, x^5, x^6\}.$$

14. a) Mỗi phần tử của S_3 là một hoán vị của $\{1, 2, 3\}$, tức là một song ánh $\{1, 2, 3\} \rightarrow \{1, 2, 3\}$. Phép toán tích trên S_3 chính là phép hợp thành ánh xạ. Các phần tử của S_3 là:

$$\begin{aligned}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} &\stackrel{k.h.}{=} (1), \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \stackrel{k.h.}{=} (1 \ 2), \\ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} &\stackrel{k.h.}{=} (1 \ 3), \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \stackrel{k.h.}{=} (2 \ 3), \\ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} &\stackrel{k.h.}{=} (1 \ 2 \ 3), \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \stackrel{k.h.}{=} (1 \ 3 \ 2).\end{aligned}$$

	(1)	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1)	(1)	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	(1)	(1 3 2)	(1 2 3)	(2 3)	(1 3)
(1 3)	(1 3)	(1 2 3)	(1)	(1 3 2)	(1 2)	(2 3)
(2 3)	(2 3)	(1 3 2)	(1 2 3)	(1)	(1 3)	(1 2)
(1 2 3)	(1 2 3)	(1 3)	(2 3)	(1 2)	(1 3 2)	(1)
(1 3 2)	(1 3 2)	(2 3)	(1 2)	(1 3)	(1)	(1 2 3)

Vì phép hợp thành có tính kết hợp nên phép toán trên S_3 có tính kết hợp. S_3 có phần tử đơn vị là (1). Căn cứ vào bảng nhân, ta thấy mọi phần tử của S_3 đều khả nghịch. Cụ thể,

$$(1)^{-1} = (1), (1 2)^{-1} = (1 2), (1 3)^{-1} = (1 3), \\ (2 3)^{-1} = (2 3), (1 2 3)^{-1} = (1 3 2), (1 3 2)^{-1} = (1 2 3).$$

Vậy S_3 là một nhóm.

b) Đặt $X = \{(1 2), (1 3), (2 3)\}$ và $Y = \{(1 2 3), (1 3 2)\}$. Căn cứ vào bảng nhân ta thấy nếu nhóm con H của S_3 chứa 2 phần tử của X hoặc 1 phần tử của X và 1 phần tử của Y thì $H = S_3$. Vậy các nhóm con của S_3 là:

$$\{(1)\}, \{(1), (1 2)\}, \{(1), (1 3)\}, \{(1), (2 3)\}, \\ \{(1), (1 2 3), (1 3 2)\}, S_3,$$

trong đó các nhóm con chuẩn tắc là $\{(1)\}, \{(1), (1 2 3), (1 3 2)\}, S_3$.

c) Vì cấp của G_3 phải là một ước chung của 24 và 30 cho nên nó phải là một ước của 6.

Ta biết rằng nhóm có cấp nhỏ hơn 6 đều là aben và nhóm cấp 6 chỉ có hai loại (sai khác đẳng cấu): aben (khi đó là nhóm cyclic) và không aben. Vậy $G_3 \cong S_3$.

15. a) Giả sử \mathbb{Q} là nhóm cyclic sinh ra bởi $\frac{m}{n}$ trong đó m và n là các số nguyên nguyên tố cùng nhau. $1 \in \mathbb{Q}$ nên tồn tại số nguyên k sao cho $1 = k \cdot \frac{m}{n}$, điều này dẫn đến sự vô lý là $n = km$.

b) Mỗi phần tử của \mathbb{Q}/\mathbb{Z} có cấp hữu hạn vì với $m, n \in \mathbb{Z}$, $n > 0$, ta có $n\left(\frac{m}{n} + \mathbb{Z}\right) = \mathbb{Z}$; trong khi mọi phần tử khác không của \mathbb{Q} đều có cấp vô hạn. Do đó \mathbb{Q}/\mathbb{Z} không thể đẳng cấu với \mathbb{Q} .

16. a) Rõ ràng $H \neq \emptyset$ và có 14 phần tử vì m có 2 cách chọn và b có 7 cách chọn.

$$\begin{pmatrix} \pm\bar{1} & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \pm\bar{1} & c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \pm\bar{1} & b \pm c \\ 0 & 1 \end{pmatrix} \in H$$

$$\begin{pmatrix} \pm\bar{1} & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \pm\bar{1} & \mp b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \bar{1} & 0 \\ 0 & 1 \end{pmatrix}$$

$$\text{hay } \begin{pmatrix} \pm\bar{1} & c \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} \pm\bar{1} & \mp b \\ 0 & 1 \end{pmatrix} \in H.$$

Vậy H là một nhóm con của $\mathrm{GL}(2, \mathbb{Z}_7)$ có 14 phần tử.

b) Ta có: $\begin{pmatrix} \bar{1} & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \bar{1} & c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \bar{1} & b+c \\ 0 & 1 \end{pmatrix},$

$$\begin{pmatrix} -\bar{1} & 0 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} \bar{1} & 0 \\ 0 & 1 \end{pmatrix} = I_2, \quad \begin{pmatrix} \bar{1} & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -\bar{1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -\bar{1} & b \\ 0 & 1 \end{pmatrix}.$$

Do đó 14 phần tử của H là:

$$I_2, \begin{pmatrix} \bar{1} & \bar{1} \\ 0 & 1 \end{pmatrix} = A, \begin{pmatrix} \bar{1} & \bar{2} \\ 0 & 1 \end{pmatrix} = A^2, \begin{pmatrix} \bar{1} & \bar{3} \\ 0 & 1 \end{pmatrix} = A^3, \begin{pmatrix} \bar{1} & \bar{4} \\ 0 & 1 \end{pmatrix} = A^4,$$

$$\begin{pmatrix} \bar{1} & \bar{5} \\ 0 & 1 \end{pmatrix} = A^5, \quad \begin{pmatrix} \bar{1} & \bar{6} \\ 0 & 1 \end{pmatrix} = A^6, \quad \begin{pmatrix} -\bar{1} & 0 \\ 0 & 1 \end{pmatrix} = B,$$

$$\begin{pmatrix} -\bar{1} & \bar{1} \\ 0 & 1 \end{pmatrix} = AB, \quad \begin{pmatrix} -\bar{1} & \bar{2} \\ 0 & 1 \end{pmatrix} = A^2B, \quad \begin{pmatrix} -\bar{1} & \bar{3} \\ 0 & 1 \end{pmatrix} = A^3B, \dots$$

$$\begin{pmatrix} -\bar{1} & \bar{4} \\ 0 & 1 \end{pmatrix} = A^4B, \quad \begin{pmatrix} -\bar{1} & \bar{5} \\ 0 & 1 \end{pmatrix} = A^5B, \quad \begin{pmatrix} -\bar{1} & \bar{6} \\ 0 & 1 \end{pmatrix} = A^6B.$$

17. a) Do $G = \langle x, y \rangle$ và $x^{-1} = x^2, y^{-1} = y$, mỗi phần tử của G có dạng:

$$x^{k_1}y^{l_1} \dots x^{k_n}y^{l_n},$$

trong đó k_i, l_i , với $1 \leq i \leq n$, là các số tự nhiên. Từ các quan hệ của G , ta có:

$$yx^3y = yy = 1 = (xy)^2 = xyxy \Rightarrow xy = yx^2.$$

Do đó các phần tử của G là y^kx^l , với $k = 0, 1$ và $l = 0, 1, 2$. Các phần tử này đôi một khác nhau nên ta có:

$$G = \{1, x, x^2, y, yx, yx^2\}.$$

Bảng nhân của G :

.	1	x	x^2	y	yx	yx^2
1	1	x	x^2	y	yx	yx^2
x	x	x^2	1	yx^2	y	yx
x^2	x^2	1	x	yx	yx^2	y
y	y	yx	yx^2	1	x	x^2
yx	yx	yx^2	y	x^2	1	x
yx^2	yx^2	y	yx	x	x^2	1

2) G có các phần tử bậc 3 là x, x^2 và các phần tử bậc 2 là y, yx, yx^2 . Căn cứ vào bảng nhân, nếu H là một nhóm con của G chứa 1 phần tử trong $\{x, x^2\}$ và 1 phần tử trong $\{y, yx, yx^2\}$ thì $H = G$. Vậy các nhóm con của G là:

$$\{1\}, \{1, x, x^2\}, \{1, y\}, \{1, yx\}, \{1, yx^2\}, G.$$

18. a) $A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, A^3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, A^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2, B^2 = I_2.$

$$BA = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = A^3B. \text{ Do đó ta có:}$$

$$G = \langle A, B \mid A^4 = B^2 = I_2, BA = A^3B \rangle.$$

$$= \{I_2, A, A^2, A^3, B, AB, A^2B, A^3B\}.$$

b) Các nhóm con của G là:

$$\begin{aligned} &\{I_2\}, \{I_2, A, A^2, A^3\}, \{I_2, A^2\}, \\ &\{I_2, B\}, \{I_2, AB\}, \{I_2, A^2B\}, \{I_2, A^3B\}, \{I_2, A^2, B, A^2B\}, G. \end{aligned}$$

19. a) Vì f_n là một toàn ánh nên tồn tại $z \in G$ sao cho $y = z^n$.

Với $x \in G$, vì f_n là một đồng cấu, ta có: $(xzx^{-1})^n = x^n z^n x^{-n}$. Từ đó:

$$xyx^{-1} = xz^n x^{-1} = (xzx^{-1})^n = x^n z^n x^{-n} = x^n yx^{-n}.$$

Vậy $x^{n-1}y = yx^{n-1}$.

b) Với $n = 3$, ta có: $x^2y = yx^2$. Ngoài ra,

$$x(yx)^2y = (xy)^3 = x^3y^3 = x(x^2y^2)y.$$

Vậy, $(yx)^2 = x^2y^2 = (x^2y)y = (yx^2)y = (yx)(xy)$. Từ đó $yx = xy$.

20. a) $1 = 1^n$ và $1^n = 1$ nên $1 \in G^{(n)}$ và $1 \in G_{(n)}$, nghĩa là $G^{(n)} \neq \emptyset$ và $G_{(n)} \neq \emptyset$. $\forall x^n, y^n \in G^{(n)}, x^n(y^n)^{-1} = x^n(y^{-1})^n = (xy^{-1})^n \in G^{(n)}$.

$\forall x, y \in G_{(n)}, x^n = y^n = 1$, nên $(xy^{-1})^n = x^n(y^n)^{-1} = 1$ hay $xy^{-1} \in G_{(n)}$. Ngoài ra, $\forall y \in G, \forall x \in G, yx^n y^{-1} = (yxy^{-1})^n \in G^{(n)}$; $\forall z \in G_{(n)}, (yzy^{-1})^n = yz^n y^{-1} = yy^{-1} = 1$ hay $yzy^{-1} \in G_{(n)}$. Vậy $G^{(n)}$ và $G_{(n)}$ là các nhóm con chuẩn tắc của G .

b) Xét ánh xạ $f : G \rightarrow G^{(n)}$ cho bởi $f(x) = x^n$. Rõ ràng f là một toàn cầu. $\text{Ker } f = \{x \in G \mid x^n = 1\} = G_{(n)}$. Do đó ta có $G/\text{Ker } f \cong \text{Im } f$ hay $G/G_{(n)} \cong G^{(n)}$.

21. a) Xét ánh xạ $\varphi : \mathbb{C}^* \rightarrow \mathbb{R}_+^*$ cho bởi $\varphi(z) = |z|$. Khi đó φ là một toàn cầu và $\text{ker } \varphi = H$, nên $\mathbb{C}^*/H \cong \mathbb{R}_+^*$.

b) Từ định nghĩa về nhóm con chuẩn tắc suy ra dễ dàng $N = f^{-1}(M) \triangleleft G$ khi $M \triangleleft H$. Xét ánh xạ $\varphi : G \rightarrow H/M$ cho bởi $\varphi(x) = f(x)M$. Khi đó φ là một toàn cầu và $\text{ker } \varphi = N$, nên $G/N \cong H/M$.

22. a) Giả sử $G = \langle a \rangle$ và $f, g \in \text{Aut}(G)$ với $f(a) = a^r$ và $g(a) = a^s$. Khi đó $(g \circ f)(a) = g(f(a)) = g(a^r) = g(a)^r = a^{sr} = a^{rs} = f(a)^s = f(a^s) = f(g(a)) = (f \circ g)(a)$. Do đó $g \circ f = f \circ g$ hay $\text{Aut}(G)$ là nhóm aben.

b) Nếu $G = \langle a \rangle$ có cấp p nguyên tố thì với mỗi tự đồng cấu nhóm của G cho bởi $f(a) = a^r$, trong đó r là số nguyên không âm, ta có $f \in \text{Aut}(G)$ khi và chỉ khi a^r là phần tử sinh của G tức là khi và chỉ khi r nguyên tố cùng nhau với p hay $r = 1, 2, \dots, p-1$. Do đó $\text{Aut}(G)$ là nhóm có cấp $p-1$. Ngoài ra, $\text{Aut}(G)$ là nhóm đẳng cấu với $Z_p^* = Z_p \setminus \{0\}$, nên $\text{Aut}(G)$ là nhóm cyclic.

23. a) Vì $G/\text{ker } f \cong f(G)$ nên $|f(G)| = |G/\text{ker } f|$ chia hết $|G|$.

b) Giả sử G có n lớp kề phân biệt là x_1H, x_2H, \dots, x_nH . Với mỗi $y \in K$ tồn tại $x \in G$ sao cho $y = f(x)$. Khi đó $x \in x_iH$ với i nào đó và $y \in f(x_i)f(H)$. Nếu $f(x_i)f(H) = f(x_j)f(H)$ thì $f(x_j)^{-1}f(x_i) = f(x')$ với $x' \in H$, nên ta có $x_j^{-1}x_i x'^{-1} \in \text{Ker } f$, mà $\text{Ker } f \subset H$, do đó $x_j^{-1}x_i \in H$ hay $x_iH = x_jH$, từ đó $i = j$. Nói cách khác K có n lớp kề phân biệt là $f(x_1)f(H), f(x_2)f(H), \dots, f(x_n)f(H)$ hay $[K : f(H)] = n$.

24. a) Với mọi $y \in G$, tồn tại duy nhất $x = g^{-1}yg$ sao cho $C_g(x) = y$, nên C_g là một song ánh. Ngoài ra, $C_g(xx') = gxx'g^{-1} = gxg^{-1} \cdot gx'g^{-1} = C_g(x)C_g(x')$. Do đó C_g là một tự đồng cấu của G . $\text{Aut}(G)$ là một nhóm với phép toán hợp thành, đơn vị là ánh xạ đồng nhất id_G , nghịch đảo của $f \in \text{Aut}(G)$ là ánh xạ ngược f^{-1} . Với mọi $f \in \text{Aut}(G)$, với mọi $g \in G$,

$$\begin{aligned} (f^{-1}C_g f)(x) &= f^{-1}(gf(x)g^{-1}) = (f^{-1}(g))x(f^{-1}(g))^{-1} \\ &= C_{f^{-1}(g)}(x) \end{aligned}$$

với mọi $x \in G$ nên $f^{-1}C_gf = C_{f^{-1}(g)} \in \text{Inn}(G)$. Do đó $\text{Inn}(G) \triangleleft \text{Aut}(G)$.

b) Dễ dàng có được $Z(G)$ là một nhóm con chuẩn tắc của G . Xét ánh xạ

$$\varphi : G \longrightarrow \text{Inn}(G)$$

xác định bởi $\varphi(g) = C_g$ thì φ là một toàn ánh và do $C_{gg'} = C_gC_{g'}$ nên φ là một toàn cầu. Ngoài ra, $C_g = id_G$ khi và chỉ khi $g \in Z(G)$ nên $Z(G) = \ker f$. Vì vậy, $G/Z(G) \cong \text{Inn}(G)$.

25. a) $\forall x \in G, \forall a \in [G, G]$, ta có $x^{-1}ax = a(a^{-1}x^{-1}ax) \in [G, G]$. Vậy $[G, G] \triangleleft G$.

Với $H \triangleleft G$, G/H là aben $\iff \forall x, y \in G, (xH)(yH) = (yH)(xH)$
 $\iff \forall x, y \in G, xyH = yxH \iff \forall x, y \in G, (yx)^{-1}xy \in H$
 $\iff \forall x, y \in G, x^{-1}y^{-1}xy \in H \iff [G, G] \subset H$. Do đó $[G, G]$ là nhóm con chuẩn tắc nhỏ nhất của G sao cho $G/[G, G]$ là aben.

$$\begin{aligned} b) [xy, z] &= (xy)^{-1}z^{-1}xyz = y^{-1}x^{-1}z^{-1}xyz \\ &= y^{-1}(x^{-1}z^{-1}xz)y(y^{-1}z^{-1}yz) = y^{-1}[x, z]y[y, z]. \end{aligned}$$

c) Nếu $[G, G] \subset Z(G)$ thì ta có

$$[xy, a] = y^{-1}[x, a]y[y, a] = [x, a]y^{-1}y[y, a] = [x, a][y, a]$$

hay $f(xy) = f(x)f(y)$, $\forall x, y \in G$. Vậy f là một đồng cấu nhóm.

$$\text{Ker } f = \{x \in G \mid [x, a] = 1\} = \{x \in G \mid xa = ax\}.$$

d) Nhóm S_3 gồm 6 phần tử:

$$\begin{aligned} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} &\stackrel{k.h.}{=} (1), \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \stackrel{k.h.}{=} (1 \ 2 \ 3), \\ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} &\stackrel{k.h.}{=} (1 \ 3 \ 2), \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \stackrel{k.h.}{=} (1 \ 2), \\ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} &\stackrel{k.h.}{=} (1 \ 3), \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \stackrel{k.h.}{=} (2 \ 3). \end{aligned}$$

Kiểm tra được rằng: $\forall x, y \in S_3$, $[x, y] = (1)$ hoặc $(1 \ 2 \ 3)$ hoặc $(1 \ 3 \ 2)$, tức là $[S_3, S_3] = \{(1), (1 \ 2 \ 3), (1 \ 3 \ 2)\} = \langle (1 \ 2 \ 3) \rangle$.

Do $[S_3, S_3] \triangleright S_3$ nên có nhóm thương $S_3/[S_3, S_3]$ và nhóm này có cấp $6/3 = 2$. Vậy $S_3/[S_3, S_3] \cong \mathbb{Z}_2$.

26. Gọi $l = \text{ord}(a^m)$ và $l' = \frac{n}{(m, n)}$. Ta có

$$a^{ml} = 1 \Rightarrow n \mid ml \Rightarrow \frac{n}{(m, n)} \mid \frac{m}{(m, n)}l.$$

Do đó $l'|l$. Mặt khác $n \mid ml'$ nên $a^{ml'} = 1$ tức là $\text{ord}(a^m)|l'$ hay $l \mid l'$.
Vậy $l = l'$.

27. a) Do $(168, 132) = 12$ nên cấp của g^{132} là $\frac{168}{12} = 14$.

b) Với $\mathbb{Z}_{140} = \langle \bar{1} \rangle$ và m là số nguyên thoả mãn $0 \leq m \leq 139$,

$$\begin{aligned}\text{ord}(m\bar{1}) = 14 &\Leftrightarrow \frac{140}{(140, m)} = 14 \Leftrightarrow (140, m) = 10 \\ &\Leftrightarrow m = 10, 30, 50, 90, 110, 130.\end{aligned}$$

Vậy các phần tử cấp 14 của nhóm cộng \mathbb{Z}_{140} là $\overline{10}, \overline{30}, \overline{50}, \overline{90}, \overline{110}, \overline{130}$.

28. a) Nếu $G = \{1\}$ thì G là cyclic. Nếu $G \neq \{1\}$, gọi a là phần tử sinh của G , thì $a^k \in G$ với k là số nguyên dương nào đó. Gọi m là số nguyên dương nhỏ nhất sao cho $a^m \in G$. Với mọi $b \in G$, ta có $b = a^n$ với số nguyên n nào đó. Theo thuật toán chia, $n = qm + r$ với $0 \leq r < m$. Khi đó $a^r = (a^m)^{-q}a^n \in G$. Do tính nhỏ nhất của m suy ra $r = 0$. Vì vậy $n = qm$ và $b = (a^m)^q$, tức là G là nhóm cyclic sinh ra bởi a^m .

b) Giả sử $|C| = n$ và $n|m$. Ta có $G = \langle a^{\frac{n}{m}} \rangle$ là nhóm con của C có cấp m . Ngoài ra, nếu H là nhóm con của C có cấp m . Giả sử $H = \langle a^s \rangle$. Khi đó $a^{sm} = (a^s)^m = 1$ nên $n \mid sm$ do đó $\frac{n}{m} \mid s$. Vì vậy $a^s \in G$ hay $H \subset G$ và suy ra $H = G$ vì $|H| = |G|$.

c) Nếu $|C| = \infty$ và $C = \langle a \rangle = \langle a^i \rangle$ thì tồn tại số nguyên j sao cho $a = (a^i)^j = a^{ij}$. Khi đó $ij = 1$, nên $i = 1$ hay $i = -1$.

d) Nếu $|C| = n < \infty$ thì a^m là phần tử sinh của C khi và chỉ khi $\text{ord}(a^m) = n$ tức là khi và chỉ khi $\frac{n}{(n, m)} = n$ hay $(n, m) = 1$.

29. Nếu $f : \mathbb{Q} \rightarrow \mathbb{Q}$ xác định bởi $f(x) = ax$ với $a \in \mathbb{Q}$ thì f là một đồng cấu nhóm. Thật vậy, $\forall x, y \in \mathbb{Q}$, $f(x+y) = a(x+y) = ax+ay = f(x) + f(y)$.

Dảo lại, nếu $f : \mathbb{Q} \rightarrow \mathbb{Q}$ là một đồng cấu nhóm thì đặt $a = f(1)$, ta có $a = f(1) = f(n \cdot \frac{1}{n}) = nf(\frac{1}{n})$ hay $f(\frac{1}{n}) = \frac{a}{n}$ với mọi số nguyên dương n . Khi đó $\forall x \in \mathbb{Q}$, $x = \frac{m}{n}$, $m \in \mathbb{Z}$, n là số nguyên dương, ta có $f(x) = f(\frac{m}{n}) = f(m \cdot \frac{1}{n}) = mf(\frac{1}{n}) = m \cdot \frac{a}{n} = a \cdot \frac{m}{n} = ax$. Rõ ràng a duy nhất sao cho $f(x) = ax$, $\forall x \in \mathbb{Q}$.

30. Ta chứng minh chỉ có một đồng cấu nhóm $f : \mathbb{Q} \rightarrow \mathbb{Q}^+$ là đồng cấu tầm thường, tức là $f(x) = 1$, $\forall x \in \mathbb{Q}$.

Đặt $m = f(1)$. Ta có $m \in \mathbb{Q}^+$ và $\forall n \in \mathbb{N}^*$,

$$m = f(1) = f\left(\frac{1}{n} + \cdots + \frac{1}{n}\right) = f\left(\frac{1}{n}\right)^n.$$

Do $f\left(\frac{1}{n}\right)$ là một số hữu tỉ và $f\left(\frac{1}{n}\right) = m^{\frac{1}{n}}$, $\forall n \in \mathbb{N}^*$, ta phải $m^{\frac{1}{n}} = 1$.

Bây giờ, $\forall x \in \mathbb{Q}$, x có biểu diễn $x = \frac{p}{q}$, với $p, q \in \mathbb{Z}$, $q > 0$ và

$$f(x) = f\left(\frac{p}{q}\right) = f\left(\frac{1}{q}\right)^p = 1^p = 1.$$

31. $\forall h, k \in H$, $\forall x \in G \setminus H$,

$$h^{-1}k^{-1} = (xhx^{-1})(xkx^{-1}) = x(hk)x^{-1} = (hk)^{-1} = k^{-1}h^{-1}.$$

Do đó $hk = kh$, $\forall h, k \in H$ hay H là một nhóm aben.

Từ điều kiện của nhóm con H , ta có ngay $H \triangleleft G$ và nhóm thương G/H có cấp 2. Do đó ta có:

$$\forall x \in G \setminus H, (xH)^2 = H \Rightarrow x^2H = H \Rightarrow x^2 \in H.$$

Giả sử $x^2 \neq 1$. Khi đó $xx^2x^{-1} = (x^2)^{-1}$ hay $x^4 = 1$ và suy ra $x^2 \in H$ có cấp 2. Điều này vô lý vì cấp của x^2 là ước của $n = |H|$, với n là một số tự nhiên lẻ. Vậy $x^2 = 1$, $\forall x \in G \setminus H$ hay mọi phần tử của $G \setminus H$ đều có cấp 2.

32. Xét phép tương ứng

$$f : \mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n : x \pmod{mn} \mapsto (x \pmod{m}, x \pmod{n}).$$

$$\begin{aligned} x \pmod{mn} = y \pmod{mn} &\Leftrightarrow x - y \equiv 0 \pmod{mn} \\ &\Leftrightarrow x - y \equiv 0 \pmod{m} \text{ và } x - y \equiv 0 \pmod{n} \\ &\Leftrightarrow x \pmod{m} = y \pmod{m} \text{ và } x \pmod{n} = y \pmod{n} \\ &\Leftrightarrow (x \pmod{m}, x \pmod{n}) = (y \pmod{m}, y \pmod{n}). \end{aligned}$$

Do đó f là một đơn ánh. Vì $|\mathbb{Z}_{mn}| = |\mathbb{Z}_m \times \mathbb{Z}_n| = mn$ nên f là một song ánh. Ngoài ra,

$$\begin{aligned} f(x \pmod{mn} + y \pmod{mn}) &= f(x + y \pmod{mn}) \\ &= (x + y \pmod{m}, x + y \pmod{n}) \\ &= (x \pmod{m}, x \pmod{n}) + (y \pmod{m}, y \pmod{n}) \end{aligned}$$

$$= f(x \text{ mod } mn) + f(y \text{ mod } mn).$$

Vậy f là một đồng cấu.

Do $\mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_6$ nên $\mathbb{Z}_3 \times \mathbb{Z}_2$ là một nhóm aben, trong khi nhóm đối xứng S_3 không aben. Vì vậy $\mathbb{Z}_3 \times \mathbb{Z}_2 \not\cong S_3$.

33. Xét ánh xạ

$$f : G \longrightarrow G/M \times G/N, x \mapsto (xM, xN)$$

$$\begin{aligned} \forall x, y \in G, f(xy) &= (xyM, xyN) = (xM \cdot yM, xN \cdot yN) \\ &= (xM, xN)(yM, yN) = f(x)f(y). \end{aligned}$$

Vậy f là một đồng cấu nhóm.

$\forall (aM, bN) \in G/M \times G/N, a = uv, b = zt, u, z \in M, v, t \in N$ (vì $G = MN$). Đặt $x = zv$ thì do $M \triangleleft G, u^{-1}z \in M, t^{-1}v \in N$, ta có

$$\begin{cases} a^{-1}x = v^{-1}u^{-1}zv = v^{-1}(u^{-1}z)v \in M \\ b^{-1}x = t^{-1}z^{-1}zv = t^{-1}v \in N \end{cases} \Rightarrow \begin{cases} xM = aM \\ xN = bN \end{cases}$$

Tức là $\exists x = zv \in G$ sao cho $f(x) = (xM, xN)$. Do đó f là một toàn cầu nhóm.

$$\begin{aligned} \text{Ker } f &= \{x \in G \mid f(x) = (xM, xN) = (M, N)\} \\ &= \{x \in G \mid x \in M \wedge x \in N\} = M \cap N. \end{aligned}$$

Vậy $G/\text{Ker } f \cong \text{Im } f$ hay $G/(M \cap N) \cong G/M \times G/N$.

34. a) Phép toán $*$ thoả mãn tính kết hợp. G có phần tử trung hoà là $(0, 0, 0)$. Nghịch đảo của $(a, b, c) \in G$ là $(-a, -b, -c - ba)$. Do đó $(G, *)$ là một nhóm. Nhóm này không aben vì

$$(1, 0, 0) * (0, 1, 0) = (1, 1, 0) \neq (1, 1, 1) = (0, 1, 0) * (1, 0, 0).$$

b) \mathbb{R}^2 có phần tử trung hoà là $(1, 0)$. Với $x, y \in \mathbb{R}$ cho trước, hệ phương trình

$$\begin{cases} xx' - yy' = 1 \\ yx' + xy' = 0 \end{cases} \text{ chỉ có nghiệm duy nhất khi } \begin{vmatrix} x & -y \\ y & x \end{vmatrix} = x^2 + y^2 \neq 0.$$

Do đó (\mathbb{R}^2, \circ) không là một nhóm vì phần tử $(0, 0)$ không nghịch.

35. f là một đồng cấu nhóm vì $\forall x, y \in \mathbb{R}$

$$f(x)*f(y) = \frac{e^x - e^{-x}}{2} \sqrt{1 + \left(\frac{e^y - e^{-y}}{2}\right)^2} + \frac{e^y - e^{-y}}{2} \sqrt{1 + \left(\frac{e^x - e^{-x}}{2}\right)^2}$$

$$\begin{aligned}
 &= \frac{e^x - e^{-x}}{2} \cdot \frac{e^y + e^{-y}}{2} + \frac{e^y - e^{-y}}{2} \cdot \frac{e^x + e^{-x}}{2} = \frac{e^{x+y} - e^{-(x+y)}}{2} \\
 &= f(x+y).
 \end{aligned}$$

f còn là một song ánh vì f có ánh xạ ngược là

$$f^{-1}(x) = \ln(x + \sqrt{x^2 + 1}).$$

Do đó f là một đẳng cấu nhóm.

36. a) Bảng nhân của $U_{22} = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}, \bar{9}, \bar{13}, \bar{15}, \bar{17}, \bar{19}, \bar{21}\}$:

.	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$	$\bar{9}$	$\bar{13}$	$\bar{15}$	$\bar{17}$	$\bar{19}$	$\bar{21}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$	$\bar{9}$	$\bar{13}$	$\bar{15}$	$\bar{17}$	$\bar{19}$	$\bar{21}$
$\bar{3}$	$\bar{3}$	$\bar{9}$	$\bar{15}$	$\bar{21}$	$\bar{5}$	$\bar{17}$	$\bar{1}$	$\bar{7}$	$\bar{13}$	$\bar{19}$
$\bar{5}$	$\bar{5}$	$\bar{15}$	$\bar{3}$	$\bar{13}$	$\bar{1}$	$\bar{21}$	$\bar{9}$	$\bar{19}$	$\bar{7}$	$\bar{17}$
$\bar{7}$	$\bar{7}$	$\bar{21}$	$\bar{13}$	$\bar{5}$	$\bar{19}$	$\bar{3}$	$\bar{17}$	$\bar{9}$	$\bar{1}$	$\bar{15}$
$\bar{9}$	$\bar{9}$	$\bar{5}$	$\bar{1}$	$\bar{19}$	$\bar{15}$	$\bar{7}$	$\bar{3}$	$\bar{21}$	$\bar{17}$	$\bar{13}$
$\bar{13}$	$\bar{13}$	$\bar{17}$	$\bar{21}$	$\bar{3}$	$\bar{7}$	$\bar{15}$	$\bar{19}$	$\bar{1}$	$\bar{5}$	$\bar{9}$
$\bar{15}$	$\bar{15}$	$\bar{1}$	$\bar{9}$	$\bar{17}$	$\bar{3}$	$\bar{19}$	$\bar{5}$	$\bar{13}$	$\bar{21}$	$\bar{7}$
$\bar{17}$	$\bar{17}$	$\bar{7}$	$\bar{19}$	$\bar{9}$	$\bar{21}$	$\bar{1}$	$\bar{13}$	$\bar{3}$	$\bar{15}$	$\bar{5}$
$\bar{19}$	$\bar{19}$	$\bar{13}$	$\bar{7}$	$\bar{1}$	$\bar{17}$	$\bar{5}$	$\bar{21}$	$\bar{15}$	$\bar{9}$	$\bar{3}$
$\bar{21}$	$\bar{21}$	$\bar{19}$	$\bar{17}$	$\bar{15}$	$\bar{13}$	$\bar{9}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$

$$\bar{7}^1 = \bar{7}, \bar{7}^2 = \bar{5}, \bar{7}^3 = \bar{13}, \bar{7}^4 = \bar{3}, \bar{7}^5 = \bar{21},$$

$$\bar{7}^6 = \bar{15}, \bar{7}^7 = \bar{17}, \bar{7}^8 = \bar{9}, \bar{7}^9 = \bar{19}, \bar{7}^{10} = \bar{1},$$

Vậy U_{22} là một nhóm cyclic sinh bởi $\bar{7}$.

b) $U_{24} = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}, \bar{13}, \bar{17}, \bar{19}, \bar{23}\}$.

$$\bar{5}^2 = \bar{25}, \bar{5}^4 = \bar{1}.$$

$$\bar{7}^2 = \bar{1}.$$

$$\bar{11}^2 = \bar{1}.$$

$$\bar{13}^2 = \bar{1}.$$

$$\bar{17}^2 = \bar{1}.$$

$$\bar{19}^2 = \bar{1}.$$

$$\bar{23}^2 = \bar{1}.$$

Vậy U_{24} không là nhóm cyclic.

37. a) Rõ ràng $0 \in R_*$, phép toán $*$ có tính kết hợp, 0 là phần tử đơn vị (do $x * 0 = 0 * x = x$) và mọi $x \in R_*$ đều khả nghịch (do định nghĩa của R_*). Do đó, R_* là một nhóm.

b) Với $x \in U(R)$, $(1-x) * (1-x^{-1}) = (1-x^{-1}) * (1-x) = 0$, nên ta có ánh xạ $f : U(R) \rightarrow R_*$ cho bởi $f(x) = 1-x$. Rõ ràng f là một song ánh. Ngoài ra, $f(x) * f(y) = (1-x) * (1-y) = (1-x) + (1-y) - (1-x)(1-y) = 1 - xy = f(xy)$. Do đó f là một đẳng cấu nhóm.

38. a) Với $g, h \in G$, nếu $g^{-1}\varphi(g) = h^{-1}\varphi(h)$ thì $\varphi(g)\varphi(h)^{-1} = gh^{-1}$ hay $\varphi(gh^{-1}) = gh^{-1}$. Từ giả thiết về φ ta phải có $gh^{-1} = 1_G$ hay $g = h$. Do đó $\{g^{-1}\varphi(g) \mid g \in G\} = G$.

b) $\forall \alpha \in G$, $\exists g \in G$ sao cho $\alpha = g^{-1}\varphi(g)$ và ta có

$$\varphi(\alpha) = \varphi(g^{-1}\varphi(g)) = \varphi(g^{-1}) \cdot \varphi(\varphi(g)) = \varphi(g)^{-1}g = (g^{-1}\varphi(g))^{-1} = \alpha^{-1}.$$

$\forall \alpha, \beta \in G$, $\varphi(\alpha\beta) = (\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1} = \varphi(\beta)\varphi(\alpha) = \varphi(\beta\alpha)$. Do đó $\alpha\beta = \beta\alpha$, $\forall \alpha, \beta \in G$ hay G là aben.

Với mọi $\alpha \in G$, $\alpha \neq 1_G$, ta có $\alpha \neq \varphi(\alpha) = \alpha^{-1}$. Như vậy G không có phần tử cấp 2. Từ đó suy ra G có cấp lẻ.

39. a) Ta có $G \subset GL(2, \mathbb{R})$. Rõ ràng $G \neq \emptyset$.

$$\forall A = \begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix}, A' = \begin{pmatrix} r' & s' \\ 0 & 1 \end{pmatrix} \in G, AA' = \begin{pmatrix} rr' & rs' + s \\ 0 & 1 \end{pmatrix} \in G,$$

$$A^{-1} = \begin{pmatrix} r^{-1} & -r^{-1}s \\ 0 & 1 \end{pmatrix} \in G.$$

Do đó G là một nhóm con của $GL(2, \mathbb{R})$, nên G là một nhóm với phép nhân ma trận.

Rõ ràng $H \neq \emptyset$.

$$\forall B = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, B' = \begin{pmatrix} 1 & t' \\ 0 & 1 \end{pmatrix} \in H, \forall A = \begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix} \in G,$$

$$BB'^{-1} = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -t' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & t - t' \\ 0 & 1 \end{pmatrix} \in H,$$

$$A^{-1}BA = \begin{pmatrix} r^{-1} & -r^{-1}s \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & r^{-1}t \\ 0 & 1 \end{pmatrix} \in H.$$

Do đó H là một nhóm con chuẩn tắc của G .

b) Xét ánh xạ $f : G \rightarrow \mathbb{R}^*$ cho bởi $f\left(\begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix}\right) = r$. Rõ ràng f là một toàn ánh. $\forall A = \begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix}, A' = \begin{pmatrix} r' & s' \\ 0 & 1 \end{pmatrix} \in G, f(AA') = f\left(\begin{pmatrix} rr' & rs' + s \\ 0 & 1 \end{pmatrix}\right) = rr' = f(A)f(A')$. Do đó f là một toàn cầu.

Do $Ker f = H, Im f = \mathbb{R}^*$ và $G/Ker f \cong Im f$, nên $G/H \cong \mathbb{R}^*$

40. a) Ta có:

$$P = \left\{ \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \mid a, b, c, d, e, f \in \mathbb{R}, a \neq 0, d \neq 0, f \neq 0 \right\}$$

là một tập con của $GL(3, \mathbb{R})$. Rõ ràng $P \neq \emptyset$. $\forall A = \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix}, A' = \begin{pmatrix} a' & b' & c' \\ 0 & d' & e' \\ 0 & 0 & f' \end{pmatrix} \in P,$

$$AA' = \begin{pmatrix} aa' & ab' + bd' & ac' + be' + cf' \\ 0 & dd' & de' + ef' \\ 0 & 0 & ff' \end{pmatrix} \in P,$$

$$A^{-1} = \begin{pmatrix} \frac{1}{a} & -\frac{b}{ad} & \frac{be}{ad} - \frac{c}{af} \\ 0 & \frac{1}{d} & -\frac{e}{df} \\ 0 & 0 & \frac{1}{f} \end{pmatrix} \in P,$$

Do đó P là một nhóm con của nhóm $GL(3, \mathbb{R})$.

$$\begin{aligned} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} &= \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

Vậy P là một nhóm không giao hoán với phép nhân ma trận.

b) $\forall A = \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \in P,$

$$A^2 = I_3 \Leftrightarrow \begin{cases} a^2 = 1 \\ d^2 = 1 \\ f^2 = 1 \\ b = -\frac{b}{ad} \\ e = -\frac{c}{df} \\ c = \frac{bc}{adf} - \frac{c}{af} \end{cases}$$

Do đó các phần tử cấp 2 trong P là:

$$\begin{aligned} & \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & e \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & c \\ 0 & -1 & e \\ 0 & 0 & 1 \end{pmatrix}; \\ & \begin{pmatrix} -1 & b & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & b & c \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & b & -\frac{bc}{2} \\ 0 & -1 & e \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & b & \frac{be}{2} \\ 0 & 1 & e \\ 0 & 0 & -1 \end{pmatrix}. \end{aligned}$$

41. a) 12 phần tử của A_4 với đơn vị ι là:

$$\begin{aligned} \iota &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}, \\ \tau_3 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \quad \tau_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, \quad \tau_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \\ \tau_6 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}, \quad \tau_7 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \quad \tau_8 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \\ \sigma_1 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}. \end{aligned}$$

Giả sử A_4 có một nhóm con H cấp 6. Do $\sigma_i^2 = \iota$ và $\tau_j^3 = \iota$ nên σ_i có cấp 2 và τ_j có cấp 3 với $i = 1, 2, 3$ và $j = 1, 2, \dots, 8$. Do H có cấp 6 nên H chứa một 3-nhóm con Sylow và một 2-nhóm con Sylow. Do đó $\tau_j \in H$ và $\sigma_i \in H$ với j và i nào đó, chẳng hạn $\tau_1 \in H$ và $\sigma_2 \in H$. Khi đó H chứa các phần tử $\iota, \tau_1, \tau_1^2 = \tau_2, \sigma_1, \sigma_1 \tau_1 = \tau_8, \tau_1 \sigma_1 = \tau_5, \tau_8^2 = \tau_7, \tau_5^2 = \tau_6$. Điều này cho biết H có ít nhất 8 phần tử, mâu thuẫn với $|H| = 6$. Vậy A_4 không chứa một nhóm con cấp 6 nào.

b) Cấp của một 2-nhóm con Sylow là 4, vì 2^2 là lũy thừa cao nhất của 2 chia hết $12 = |A_4|$. Do không có τ_j nào có thể là phần tử

của một 2-nhóm con Sylow (vì chúng đều có cấp là 3), $\sigma_i\sigma_k = \sigma_l$ với $i, k, l \in \{1, 2, 3\}$, $\sigma_i^2 = \iota$ với $i = 1, 2, 3$ và $\iota, \sigma_1, \sigma_2, \sigma_3$ là bốn phần tử duy nhất trong A_4 có cấp ước của 4, ta có 2-nhóm con Sylow duy nhất là $P = \{\iota, \sigma_1, \sigma_2, \sigma_3\}$.

Cấp của một 3-nhóm con Sylow là 3. Các tập

$$\{\iota, \tau_1, \tau_1^2\}, \{\iota, \tau_3, \tau_3^2\}, \{\iota, \tau_5, \tau_5^2\}, \{\iota, \tau_7, \tau_7^2\}$$

là các nhóm con cấp 3. Số các 3-nhóm con Sylow là $s_3 = 1 + 3k$, với $k \in \mathbb{Z}$, phải chia hết cho 12. Rõ ràng $k \neq 0$, và nếu $k > 1$ thì s_3 không chia hết 12. Do đó $k = 1$ và có đúng bốn 3-nhóm con Sylow như trên.

42. a) Giả sử $|H| = p^t$, $t \geq 0$. Theo định lý Lagrange, $p^t \mid p^r m$. Vì $p \nmid m$ nên $t \leq r$. Do $P \subset H$ và $|P| = p^r$, ta có $t = r$ và vì vậy $P = H$.

b) Với mỗi $g \in G$, ánh xạ $P \rightarrow g^{-1}Pg : x \mapsto g^{-1}xg$ là một song ánh, nên $|g^{-1}Pg| = |P| = p^r$. Do đó $g^{-1}Pg$ là p -nhóm con Sylow, với mỗi $g \in G$. Do G chỉ có p -nhóm con Sylow duy nhất là P nên $g^{-1}Pg = P$, $\forall g \in G$ hay $P \triangleleft G$.

43. a) Số q -nhóm con Sylow cấp q của G là $s_q = 1 + kq$, với $k \geq 0$ nào đó. Ngoài ra, $1 + kq$ chia hết pq , nên có bốn khả năng xảy ra: $1 + kq = q$ hoặc $1 + kq = p$ hoặc $1 + kq = pq$ hoặc $1 + kq = 1$. Vì q không chia hết $1 + kq$, chỉ còn hai khả năng $1 + kq = p$ hoặc $1 + kq = 1$. Vì $q > p$ nên $1 + kq \neq p$ và do đó $1 + kq = 1$. Vậy có đúng một nhóm con cấp q .

b) Số p -nhóm con Sylow cấp p của G là $s_p = 1 + kp$, với $k \geq 0$ nào đó. Lập luận như trên, ta có hai khả năng xảy ra: $1 + kp = 1$ hoặc $1 + kp = q$. Trường hợp cuối là không đúng theo giả thiết, nên chỉ có một nhóm con cấp p của G .

Gọi H là nhóm con cấp q và K là nhóm con cấp p của G . Khi đó với $h \in H$, $k \in K$, $h \neq 1$, $k \neq 1$, ta có $H = \langle h \rangle \triangleleft G$ và $K = \langle k \rangle \triangleleft G$. Ngoài ra, $H \cap K = \{1\}$ vì các phần tử khác đơn vị của H có cấp q và của K có cấp p . Do

$$\begin{aligned} h^{-1}k^{-1}hk &= h^{-1}(k^{-1}hk) \in H \text{ vì } H \triangleleft G \\ &= (h^{-1}k^{-1}h)k \in K \text{ vì } K \triangleleft G \end{aligned}$$

nên $h^{-1}k^{-1}hk = 1$ hay $hk = kh$. Theo định lý Lagrange, cấp của hk là p , q hoặc pq . Nhưng $(hk)^p = h^pk^p$ vì h giao hoán với k , vì vậy $(hk)^p = h^p \neq 1$. Tương tự $(hk)^q = k^q \neq 1$. Vậy cấp của hk là pq hay G là nhóm cyclic sinh bởi hk .

BÀI TẬP CHƯƠNG II – VÀNH

1. Cho S là một tập hợp, ký hiệu $\mathcal{P}(S)$ là tập gồm tất cả các tập con của S . Chứng tỏ rằng $\mathcal{P}(S)$ với 2 phép toán cộng và nhân như sau:

$$A + B = (A \cup B) \setminus (A \cap B), \quad AB = A \cap B, \quad \forall A, B \in \mathcal{P}(S)$$

là một vành giao hoán có đơn vị.

2. Cho R là một vành, \mathbb{Z} là vành các số nguyên, trên tập $\mathbb{Z} \times R$ ta định nghĩa 2 phép toán cộng và nhân như sau:

$$(m, x) + (n, y) = (m + n, x + y), \quad (m, x)(n, y) = (mn, my + nx + xy).$$

Chứng minh rằng $\mathbb{Z} \times R$ với 2 phép toán này là một vành có đơn vị và R đảng cấu với một iđéan của vành này.

3. Cho S là một tập hợp, R là một vành và f là một song ánh từ R lên S . Chứng minh rằng S với 2 phép toán:

$$a + b = f(f^{-1}(a) + f^{-1}(b)), \quad ab = f(f^{-1}(a)f^{-1}(b)), \quad \forall a, b \in S$$

là một vành và f là một đảng cấu vành. Dùng điều này để chứng minh rằng một vành bất kỳ có đơn vị 1 cũng còn là một vành đối với 2 phép toán:

$$a \oplus b = a + b - 1, \quad a * b = a + b - ab.$$

4. a) Cho R là một vành. Chứng minh rằng

$$Z(R) = \{a \in R \mid ax = xa, \quad \forall x \in R\}$$

là một vành con giao hoán của R gọi là tâm của R . Nếu R là một thể thì $Z(R)$ có cấu trúc gì?

b) Xác định tâm của vành $M(3, \mathbb{R})$ các ma trận vuông cấp 3 hệ số thực.

5. Một vành R được gọi là một vành Boole nếu với mỗi $a \in R$, $a^2 = a$. Cho R là một vành Boole. Chứng minh rằng:

a) R có đặc số 2.

b) R là một vành giao hoán.

c) Nếu R không có ước đa 0 thì hoặc $R = \{0\}$ hoặc R chỉ có hai phần tử.

6. Cho R là vành có đơn vị $1 \neq 0$ và $x, y \in R$. Chứng minh rằng:
- Nếu xy và yx khả nghịch thì x và y khả nghịch.
 - Nếu R không có ước của không và xy khả nghịch thì x và y khả nghịch.
7. Cho R là vành có đơn vị $1 \neq 0$.
- Chứng minh rằng nếu $a \in R$, $a \neq 0$, có nghịch đảo trái thì a không là ước của 0 bên trái và điều ngược lại vẫn đúng nếu $a \in aRa$.
 - Với $a, b \in R$, chứng minh rằng nếu $1 - ba$ khả nghịch trái thì $1 - ab$ cũng khả nghịch trái.
8. Cho R là vành hữu hạn. Chứng minh rằng
- Nếu R không có ước của không thì nó có đơn vị và mọi phần tử khác không của R đều khả nghịch.
 - Nếu R có đơn vị thì mọi phần tử khả nghịch một phía trong R đều khả nghịch.
9. Cho R là một vành. Một phần tử x của R được gọi là lũy linh nếu tồn tại $n \in \mathbb{N}^*$ sao cho $x^n = 0$. Chứng minh rằng:
- Nếu x, y lũy linh và giao hoán thì $x + y$ cũng là lũy linh.
 - Nếu x lũy linh và $xy = yx$ thì xy cũng là lũy linh.
 - Nếu x lũy linh thì $1 - x$ khả nghịch và tính $(1 - x)^{-1}$.
10. Cho p là một số nguyên tố. Chứng minh rằng tập hợp các số hữu tỉ có dạng m/n , trong đó n nguyên tố với p , là một miền nguyên. Tìm trường các thương của miền nguyên này.
11. Chứng minh rằng mọi miền nguyên hữu hạn đều là trường.
12. Cho R là một vành giao hoán, khác không và có đơn vị. Chứng minh rằng các điều sau là tương đương:
- R là một trường.
 - R chỉ có hai idéan là $\{0\}$ và R .
 - Mọi đồng cấu khác không từ vành R vào một vành khác không đều là đơn cấu.
13. Chứng minh rằng tập hợp các ma trận có dạng $\begin{pmatrix} a & b \\ 3b & a \end{pmatrix}$, với a, b là những số hữu tỉ tùy ý, là một trường đối với phép cộng và phép nhân ma trận, trường này đẳng cấu với trường $A = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$, \mathbb{Q} là trường các số hữu ti.

14. Chứng minh rằng tập hợp các ma trận có dạng $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, với a, b là những số thực tùy ý, là một trường đối với phép cộng và phép nhân ma trận, trường này đẳng cấu với trường \mathbb{C} các số phức.

15. a) Cho p là một số nguyên tố. Ký hiệu

$$\mathbb{Q}(\sqrt{p}) = \{a + b\sqrt{p} \mid a, b \in \mathbb{Q}\},$$

trong đó \mathbb{Q} là trường các số hữu tỉ. Chứng minh rằng $\mathbb{Q}(\sqrt{p})$ là một trường (trường con của trường \mathbb{R} các số thực).

b) Chứng minh rằng trường $\mathbb{Q}(\sqrt{7})$ không đẳng cấu với trường $\mathbb{Q}(\sqrt{11})$.

16. Hãy tìm các tự đồng cấu của trường \mathbb{F} :

a) \mathbb{F} là trường \mathbb{Q} các số hữu tỉ.

b) \mathbb{F} là trường \mathbb{R} các số thực.

c) \mathbb{F} là trường \mathbb{Z}_p các số nguyên modulo p , với p là một số nguyên tố.

d) \mathbb{F} là trường \mathbb{C} các số phức và chúng giữ nguyên các số thực.

17. Trên vành $M(2, \mathbb{C})$ các ma trận vuông cấp 2 hệ số trên trường các số phức \mathbb{C} , xét tập con

$$\mathcal{Q} = \left\{ \begin{pmatrix} a & b \\ -b & \bar{a} \end{pmatrix} \mid a, b \in \mathbb{C} \right\}.$$

a) Chứng minh rằng \mathcal{Q} là một thể con của vành $M(2, \mathbb{C})$.

b) Đặt $I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. Dòng nhất số thực a với $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in \mathcal{Q}$. Chứng minh rằng $I^2 = J^2 = K^2 = -1$, $IJ = -JI = K$, $JK = -KJ = I$, $KI = -IK = J$ và mọi phần tử của \mathcal{Q} đều có dạng:

$$a_1 + a_2I + b_1J + b_2K, a_1, a_2, b_1, b_2 \in \mathbb{R}.$$

(Thể \mathcal{Q} được gọi là thể quaternion.)

18. Cho K là một thể và $x, y \in K \setminus \{0\}$ sao cho $x + y = -1$ và $x^{-1} + y^{-1} = 1$. Chứng minh rằng:

$$xy = -1, \quad x^4 + y^4 = 7.$$

(Ở đây ta ký hiệu n thay cho $n1_K$, với $n \in \mathbb{Z}$ và 1_K là đơn vị của K .)

19. Tồn tại hay không một thể K sao cho các nhóm K với phép cộng và $K \setminus \{0\}$ với phép nhân đẳng cấu với nhau?

20. Ký hiệu T là vành tất cả các ma trận tam giác dưới cấp 3 trên \mathbb{Z} các số nguyên. Đặt

$$I = \left\{ \begin{pmatrix} 0 & 0 & 0 \\ a & 0 & 0 \\ b & 2c & 0 \end{pmatrix} \mid a, b, c \in \mathbb{Z} \right\},$$

$$J = \left\{ \begin{pmatrix} 0 & 0 & 0 \\ l & 0 & 0 \\ 2m & 2n & 0 \end{pmatrix} \mid l, m, n \in \mathbb{Z} \right\}.$$

Chứng minh rằng I là iđéan 2 phía của T , J là iđéan 2 phía của I và J là iđéan phải của T nhưng không là iđéan trái.

- 21. Xét vành \mathbb{Z} các số nguyên.

a) Hãy tìm tất cả các iđéan của vành \mathbb{Z} .

b) Chứng tỏ rằng mọi dãy tăng các iđéan của \mathbb{Z} đều dừng, tức là nếu $I_1 \subset I_2 \subset \dots \subset I_n \subset \dots$ là dãy các iđéan của \mathbb{Z} thì tồn tại số nguyên i sao cho với mọi j lớn hơn i thì $I_j = I_i$.

Đối với dãy giảm các iđéan của \mathbb{Z} thì thế nào?

22. Cho R và S là các vành có đơn vị. Chứng minh rằng M là một iđéan của vành tích $R \times S$ khi và chỉ khi $M = I \times J$, trong đó I và J lần lượt là các iđéan của R và S .

Tìm các iđéan của các vành tích \mathbb{Z}^2 , \mathbb{R}^2 , trong đó \mathbb{Z} và \mathbb{R} lần lượt là vành các số nguyên và các số thực.

23. Cho R là một vành giao hoán có đơn vị.

a) Chứng tỏ mọi iđéan cực đại của R đều là iđéan nguyên tố.

b) Giả sử R có tính chất: $\forall x \in R$ tồn tại số tự nhiên $n > 1$ sao cho $x^n = x$. Chứng tỏ mọi iđéan nguyên tố cũng là iđéan cực đại.

24. Ký hiệu $\mathbb{Z}[i] = \{a + ib \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$, trong đó \mathbb{C} là trường các số phức và \mathbb{Z} là vành các số nguyên. Với $u \in \mathbb{Z}[i]$, ký hiệu $(u) = \{ux \mid x \in \mathbb{Z}[i]\}$. Chứng minh:

a) $\mathbb{Z}[i]$ là vành con của \mathbb{C} và (u) là iđéan của $\mathbb{Z}[i]$.

b) Vành thương $\mathbb{Z}[i]/(2)$ không phải là trường.

c) Vành thương $\mathbb{Z}[i]/(3)$ là trường có 9 phần tử.

25. Cho R là một vành giao hoán và I là một iđéan sinh ra bởi phần tử $a \in R$. Chứng minh rằng:

$$I = \begin{cases} \{ra \mid r \in R\} & \text{nếu } R \text{ có đơn vị} \\ \{ra + na \mid r \in R \text{ và } n \in \mathbb{Z}\} & \text{nếu } R \text{ không có đơn vị} \end{cases}$$

26. Ký hiệu $M(2, \mathbb{F})$ là vành các ma trận vuông cấp 2 hệ số trên trường \mathbb{F} . Chứng tỏ rằng:

a) Tập hợp $\left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in M(2, \mathbb{F}) \mid a, b \in \mathbb{F} \right\}$ là 1 iđéan phải mà không là iđéan trái của $M(2, \mathbb{F})$.

b) Vành $M(2, \mathbb{Z}_2)$ là một vành đơn nghĩa là $M(2, \mathbb{Z}_2)$ không có iđéan nào khác ngoài iđéan không và chính nó (\mathbb{Z}_2 là trường các số nguyên mod 2).

27. Cho R là một vành khác không, không có ước của không và sao cho mọi nhóm con của nhóm cộng R là một iđéan của R . Chứng minh rằng R đẳng cấu với một vành con của vành \mathbb{Z} các số nguyên hoặc R đẳng cấu với vành \mathbb{Z}_p các số nguyên môđulô p với p là một số nguyên tố.

28. Xét $\mathcal{M} = M(n, \mathbb{R})$ là vành các ma trận vuông cấp n hệ số thực. Chứng minh rằng:

a) Ma trận A là ước (bên trái và bên phải) của không trong vành \mathcal{M} khi và chỉ khi $|A| = 0$.

b) Tập hợp \mathcal{N} tất cả ma trận mà từ dòng thứ hai trở đi đều bằng không là một vành con của \mathcal{M} và mọi ma trận khác không của \mathcal{N} đều là ước bên phải của không trong vành \mathcal{N} . Hãy xét xem những ma trận nào không phải là ước bên trái của không trong vành \mathcal{N} .

c) Trong vành \mathcal{N} tồn tại vô số đơn vị trái.

29. Xét vành \mathbb{Z}_n các số nguyên môđulô n .

a) Tìm tất cả các đồng cấu vành từ \mathbb{Z}_{72} vào \mathbb{Z}_{30} .

b) Tìm ảnh và hạt nhân của từng đồng cấu vành ở câu a).

30. Cho I và J là các iđéan của vành giao hoán có đơn vị R và ánh xạ $\phi : R \longrightarrow R/I \times R/J$ xác định bởi $\phi(r) = (r+I, r+J)$. Chứng minh rằng:

a) ϕ là một đồng cấu vành và $\text{Ker } \phi = I \cap J$.

b) Nếu $I + J = R$ thì ϕ là một toàn cầu và

$$R/IJ \cong R/I \times R/J.$$

31. Cho S là vành thương $\mathbb{Z}_2[x]/(x^3 + x)$.
- Lập bảng nhân của S .
 - Tìm các phần tử khả nghịch của S .
32. Chứng minh rằng iđêan chính $(x^2 - x + 1)$ là iđêan cực đại của vành $\mathbb{R}[x]$ với \mathbb{J} là trường các số thực. Từ đó suy ra vành thương $\mathbb{R}[x]/(x^2 - x + 1)$ là một trường.
33. Xét vành $\mathbb{Z}[x]$ các đa thức hệ số nguyên. Ký hiệu I là iđêan của $\mathbb{Z}[x]$ sinh bởi 7 và $x - 5$. Chứng minh rằng:
- $$\mathbb{Z}[x]/I \cong \mathbb{Z}_7.$$
34. Xét vành \mathbb{C} các số phức và $a = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} \in \mathbb{C}$. Chứng tỏ rằng tập hợp
- $$S = \{m + na + pa^2 + qa^3 \mid m, n, p, q \in \mathbb{Z}\}$$
- là vành con của \mathbb{C} sinh bởi a . S có là một iđêan của \mathbb{C} không?
35. Cho miền nguyên D có đơn vị 1 và 1 có cấp n . Chứng tỏ rằng:
- n là một số nguyên tố.
 - Ánh xạ $\varphi : D \longrightarrow D$ cho bởi $\varphi(x) = x^n$ là một đồng cấu vành.

TRẢ LỜI VÀ HƯỚNG DẪN GIẢI BÀI TẬP
CHƯƠNG II – VÀNH

1. Ta có hiệu đối xứng $A + B = (A \setminus B) \cup (B \setminus A)$ và

- | | |
|----------------------------------|--|
| a) $A + A = \emptyset$, | b) $A + \emptyset = A$, |
| c) $A + B = B + A$, | d) $A + B = (A \cup B) \setminus (A \cap B)$, |
| e) $(A + B) + C = A + (B + C)$, | f) $A(B + C) = AB + AC$. |

Gọi p, q, r tương ứng là các mệnh đề $x \in A, x \in B, x \in C$. Khi đó $x \in A + B$ chính là mệnh đề tuyển loại (XOR) $p \oplus q$. Bảng giá trị chân lý sau cho các kết quả câu d) từ cột 6 và 7, câu e) từ cột 8 và 10, câu f) từ cột 11 và 13.

Ta còn có: g) $AB = BA$, h) $(AB)C = A(BC)$, i) $AS = A$,

p	q	r	$p \vee q$	$p \wedge q$	$(p \vee q) \wedge (\bar{p} \wedge \bar{q})$	$p \oplus q$
0	0	0	0	0	0	0
0	0	1	0	0	0	0
0	1	0	1	0	1	1
0	1	1	1	0	1	1
1	0	0	1	0	1	1
1	0	1	1	0	1	1
1	1	0	1	1	0	0
1	1	1	1	1	0	0

$(p \oplus q) \oplus r$	$q \oplus r$	$p \oplus (q \oplus r)$	$p \wedge (q \oplus r)$	$p \wedge r$	$(p \wedge q) \oplus (p \wedge r)$
0	0	0	0	0	0
1	1	1	0	0	0
1	1	1	0	0	0
0	0	0	0	0	0
1	0	1	0	0	0
0	1	0	1	1	1
0	1	0	1	0	1
1	0	1	0	1	0

Vậy $\mathcal{P}(S)$ với phép cộng (hiệu đối xứng) và phép nhân (phép giao) là một vành giao hoán có đơn vị.

2. Dễ dàng có được $\mathbb{Z} \times R$ với phép cộng là một nhóm aben. Phép nhân trên $\mathbb{Z} \times R$ có tính kết hợp và phân phối đối với phép cộng. Thật vậy, $\forall (m, x), (n, y), (p, z) \in \mathbb{Z} \times R$,

$$\begin{aligned}
 ((m, x)(n, y))(p, z) &= (mn, my + nx + xy)(p, z) \\
 &= (mnp, mnz + pmy + pnx + pxy + myz + nxz + xyz) \\
 &= (mnp, mnz + mpy + myz + npx + nxz + pxy + xyz) \\
 &= (m, x)(np, nz + py + yz) \\
 &= (m, x)((n, y)(p, z)), \\
 (m, x)((n, y) + (p, z)) &= (m, x)(n + p, y + z) \\
 &= (mn + mp, my + mz + nx + px + xy + xz) \\
 &= (mn, my + nx + xy) + (mp, mz + px + xz) \\
 &= (m, x)(n, y) + (m, x)(p, z).
 \end{aligned}$$

Ngoài ra $\mathbb{Z} \times R$ có phần tử đơn vị là $(1, 0)$. Do đó $\mathbb{Z} \times R$ là một vành có đơn vị. Đặt $I = \{(0, x) \in \mathbb{Z} \times R\}$ thì I là một iđéan của $\mathbb{Z} \times R$. Xét ánh xạ

$$f : R \longrightarrow \mathbb{Z} \times R : x \mapsto (0, x).$$

Rõ ràng f là một đơn ánh. Ngoài ra, $\forall x, y \in R$,

$$\begin{aligned}
 f(x + y) &= (0, x + y) = (0, x) + (0, y) = f(x) + f(y), \\
 f(xy) &= (0, xy) = (0, x)(0, y) = f(x)f(y).
 \end{aligned}$$

Vậy f là một đơn cấu, nghĩa là ta có đẳng cấu vành $R \cong \text{Im } f = I$.

3. Vì R là một vành với phần tử không là 0_R nên $\forall a, b, c \in S$,

$$\begin{aligned}
 * a + b &= f(f^{-1}(a) + f^{-1}(b)) = f(f^{-1}(b) + f^{-1}(a)) = b + a \\
 * (a + b) + c &= f(f^{-1}(a + b) + f^{-1}(c)) \\
 &= f(f^{-1}(f(f^{-1}(a) + f^{-1}(b))) + f^{-1}(c)) = f(f^{-1}(a) + f^{-1}(b) + \\
 &\quad f^{-1}(c)) \\
 &= f(f^{-1}(a) + f^{-1}(f(f^{-1}(b) + f^{-1}(c)))) = f(f^{-1}(a) + f^{-1}(b + c)) \\
 &= a + (b + c) \\
 * \text{với } 0_S &= f(0_R), a + 0_S = f(f^{-1}(a) + f^{-1}(0_S)) \\
 &\quad = f(f^{-1}(a) + 0_R) = f(f^{-1}(a)) = a \\
 * \text{với } -a &= f(-f^{-1}(a)), a + (-a) = f(f^{-1}(a) + f^{-1}(f(-f^{-1}(a))))
 \end{aligned}$$

$$\begin{aligned}
 &= f(f^{-1}(a) + (-f^{-1}(a))) = f(0_R) = 0_S \\
 * (ab)c &= f(f^{-1}(ab)f^{-1}(c)) = f(f^{-1}(f(f^{-1}(a)f^{-1}(b)))f^{-1}(c)) \\
 &= f(f^{-1}(a)f^{-1}(b)f^{-1}(c)) = f(f^{-1}(a)f^{-1}(f(f^{-1}(b)f^{-1}(c)))) \\
 &= f(f^{-1}(a)f^{-1}(bc)) = a(bc). \\
 * a(b+c) &= f(f^{-1}(a)f^{-1}(b+c)) = f(f^{-1}(a)f^{-1}(f(f^{-1}(b) + \\
 &\quad f^{-1}(c)))) \\
 &= f(f^{-1}(a)(f^{-1}(b) + f^{-1}(c))) = f(f^{-1}(a)f^{-1}(b) + f^{-1}(a)f^{-1}(c)) \\
 &= f(f^{-1}(f(f^{-1}(a)f^{-1}(b)))) + f^{-1}(f(f^{-1}(a)f^{-1}(c))) \\
 &= f(f^{-1}(ab) + f^{-1}(ac)) = ab + ac. \text{ Tương tự } (b+c)a = ba + ca \\
 \text{Vậy } S &\text{ là một vành. Do } \eta \text{ là một song ánh và } f(x+y) = f(x)+f(y), \\
 f(xy) &= f(x)f(y), \forall x, y \in R \text{ nên } f \text{ là một đẳng cấu.} \\
 \text{Bây giờ, nếu } R &\text{ là vành có đơn vị 1 thì với song ánh } f : R \longrightarrow R \\
 \text{cho bởi } f(a) &= 1 - a \text{ (khi đó } f^{-1}(a) = 1 - a), R \text{ cũng là vành với hai} \\
 \text{phép toán} &
 \end{aligned}$$

$$\begin{aligned}
 a \oplus b &= f^{-1}(f(a) + f(b)) = 1 - (1 - a + 1 - b) = a + b - 1 \\
 ab &= f^{-1}(f(a)f(b)) = 1 - ((1 - a)(1 - b)) = a + b - ab.
 \end{aligned}$$

4. a) $\forall x \in R, 0x = x0 (= 0)$ hay $0 \in Z(R)$, nên $Z(R) \neq \emptyset$. $\forall a, b \in Z(R)$,

$$\begin{aligned}
 (a - b)x &= ax - bx = xa - xb = x(a - b), \forall x \in R \text{ nên } a - b \in Z(R). \\
 (ab)x &= a(bx) = a(xb) = (ax)b = (xa)b = x(ab), \forall x \in R \text{ nên} \\
 ab &\in Z(R).
 \end{aligned}$$

Rõ ràng $ab = ba, \forall a, b \in Z(R)$.

Vậy $Z(R)$ là một vành con giao hoán của R .

Với giả thiết R là một thể, $\forall x \in R, 1x = x1 (= x)$, do đó $1 \in Z(R)$; ngoài ra, $\forall a \in Z(R), a \neq 0, \exists a^{-1} \in R, aa^{-1} = 1$; do $xa = ax$, ta có $a^{-1}x = xa^{-1}$ hay $a^{-1} \in Z(R)$. Điều này cho biết $Z(R)$ là một vành giao hoán có đơn vị và mọi phần tử khác 0 của nó đều có nghịch đảo trong nó, do đó $Z(R)$ là một trường.

$$\text{b)} Z(M(3, \mathbb{R})) = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix} \mid a \in \mathbb{R} \right\}.$$

5. a) Với mọi $a \in R, 2a = a+a = (a+a)^2 = a^2 + 2a^2 + a^2 = 4a^2 = 4a$, do đó $2a = 0$. Vậy R có đặc số 2. Từ đó suy ra $a = -a, \forall a \in R$.

b) Với mọi $a, b \in R, a+b = (a+b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b$, do đó $ab + ba = 0$ hay $ab = -ba = ba$. Vậy R là một vành giao hoán.

c) Với mọi $a, b \in R$, $ab(a+b) = a^2b + ab^2 = ab + ab = 2ab = 0$, do đó hoặc $ab = 0$ hoặc $a+b = 0$. Nếu $ab = 0$ thì $a = 0$ hoặc $b = 0$. Trong trường hợp này vành R chỉ có một phần tử 0. Nếu $ab \neq 0$ (tức là $a \neq 0$ và $b \neq 0$) thì $a+b = 0$ hay $b = -a = a$. Khi đó R chỉ có hai phần tử.

6. a) Giả sử a và b lần lượt là phần tử nghịch đảo của xy và yx , nghĩa là

$$a(xy) = (xy)a = b(yx) = (yx)b = 1.$$

Đặt $x' = by$, $x'' = ya$, $y' = ax$, $y'' = xb$ thì $x'x = xx'' = 1$ và $y'y = yy'' = 1$. Do đó $x' = x''$ và $y' = y''$ lần lượt là phần tử nghịch đảo của x và y .

b) Giả sử a là phần tử nghịch đảo của xy , nghĩa là $a(xy) = (xy)a = 1$. Ta có $x \neq 0$ và $y \neq 0$, vì nếu $x = 0$ hay $y = 0$ thì $xy = 0$ nên xy không có nghịch đảo. Đặt $x' = ya$ và $y' = ax$ thì $xx' = y'y = 1$. Khi đó

$$x(x'x - 1) = xx'x - x = 1x - x = 0 \Rightarrow x'x - 1 = 0 \Rightarrow x'x = 1,$$

do R không có ước của không và $x \neq 0$. Vậy x' là phần tử nghịch đảo của x . Tương tự y' là phần tử nghịch đảo của y .

7. a) Giả sử $ba = 1$. Khi đó nếu $ac = 0$ thì $c = (ba)c = b(ac) = b0 = 0$. Do đó a không là ước của 0 bên trái.

Giả sử $a = ara$ với $r \in R$ và a không là ước của 0 bên trái. Khi đó $a(1 - ra) = a - ara = 0$ nên ta có $1 - ra = 0$ hay $ra = 1$. Do đó a có nghịch đảo trái là r .

b) Nếu tồn tại $c \in R$ sao cho $c(1 - ba) = 1$ thì $c(1 - ba)b = b$ hay $cb(1 - ab) = b$. Khi đó $1 = ab + (1 - ab) = acb(1 - ab) + (1 - ab) = (acb + 1)(1 - ab)$. Do đó $1 - ab$ khả nghịch trái.

8. a) Với $a \in R$, $a \neq 0$, xét ánh xạ

$$f_a : R \longrightarrow R : x \mapsto ax.$$

f_a là một đơn ánh. Thật vậy $\forall x, y \in R$, $ax = ay$ kéo theo $a(x - y) = 0$ nên $x - y = 0$ vì R là vành không có ước của không và $a \neq 0$. Do R là hữu hạn nên f_a là một song ánh. Vì vậy, với $a \in R$ tồn tại $e \in R$ sao cho $f_a(e) = ae = a$. Ta chứng minh e là đơn vị của R .

$\forall x \in R$, $a(ex - x) = (ae)x - ax = ax - ax = 0$, vì $a \neq 0$ nên $ex - x = 0$ hay $ex = x$. Từ đó $ea = a$ và $(xe - x)a = x(ea) - xa = xa - xa = 0$, do đó $xe - x = 0$ hay $xe = x$.

Vì f_a là song ánh nên với $e \in R$, tồn tại $a' \in R$ sao cho $f_a(a') = aa' = e$. Ta có $a(a'a - e) = (aa')a - ae = ea - ae = 0$ nên $a'a = e$. Vậy a' là phần tử nghịch đảo của a .

b) Giả sử a có nghịch đảo trái là a' , nghĩa là $a'a = e$. Xét ánh xạ

$$f_a : R \rightarrow R : x \mapsto ax.$$

f_a là một đơn ánh. Thật vậy, $\forall x, y \in R$, $ax = ay$ kéo theo $a'(ax) = a'(ay)$, do đó $x = y$. Do R là hữu hạn nên f_a là một song ánh. Khi đó với đơn vị e của R , tồn tại $a'' \in R$ sao cho $f_a(a'') = aa'' = e$, tức là a có nghịch đảo phải là a'' . Tương tự nếu a có nghịch đảo phải thì a có nghịch đảo trái nên a khả nghịch.

9. a) Tồn tại $n, p \in \mathbb{N}^*$ sao cho $x^n = y^p = 0$. Theo công thức nhị thức Newton:

$$\begin{aligned} (x+y)^{n+p-1} &= \sum_{k=0}^{n+p-1} C_{n+p-1}^k x^k y^{n+p-1-k} \\ &= (\sum_{k=0}^{n-1} C_{n+p-1}^k x^k y^{n-1-k}) y^p \\ &\quad - x^n (\sum_{k=n}^{n+p-1} C_{n+p-1}^k x^{k-n} y^{n+p-1-k}) = 0. \end{aligned}$$

Do đó $x+y$ là lũy linh.

b) Nếu $x^n = 0$ thì $(xy)^n = x^n y^n = 0$. Do đó xy là lũy linh.

c) Nếu $x^n = 0$, ký hiệu $y = \sum_{k=0}^{n-1} x^k$, ta có $(1-x)y = y(1-x) = 1 - x^n = 1$. Do đó $1-x$ khả nghịch và $(1-x)^{-1} = y$.

10. Đặt $A = \left\{ \frac{m}{n} \in \mathbb{Q} \mid (n, p) = 1 \right\}$. Ta có $A \neq \emptyset$ vì $\mathbb{Z} \subset A$.

$$\forall \frac{m_1}{n_1}, \frac{m_2}{n_2} \in A, \frac{m_1}{n_1} - \frac{m_2}{n_2} = \frac{m_1 n_2 - m_2 n_1}{n_1 n_2} \in A,$$

$$\frac{m_1}{n_1} \cdot \frac{m_2}{n_2} = \frac{m_1 m_2}{n_1 n_2} \in A,$$

vì $(n_1, p) = 1$ và $(n_2, p) = 1$ nên $(n_1 n_2, p) = 1$.

Vậy A là một vành con của \mathbb{Q} , nên A là một miền nguyên.

Gọi \bar{A} là trường các thương của A thì do $A \supset \mathbb{Z}$ nên $\bar{A} \supset \mathbb{Q}$, mặt khác vì $A \subset \mathbb{Q}$ nên $\bar{A} \subset \mathbb{Q}$. Vậy $\bar{A} = \mathbb{Q}$.

11. Cho R là một miền nguyên hữu hạn, giả sử $R = \{0, a_1, a_2, \dots, a_n\}$. Khi đó các phần tử của $R^* = \{a_1, a_2, \dots, a_n\}$ thoả mãn luật giàn ước. Do đó $R^* = \{a_1a_1, a_1a_2, \dots, a_1a_n\}$. Vì $a_1 \in R^*$ nên tồn tại k sao cho $a_1a_k = a_1$. Đặt $e = a_k$, với $1 \leq i \leq n$ ta có $a_1(ea_i) = (a_1e)a_i = a_1a_i$, suy ra $ea_i = a_i$ hay e là phần tử đơn vị của R . Với mọi $a_j \in R^*$, $R^* = \{a_1a_j, a_2a_j, \dots, a_na_j\}$. Vì $e \in R^*$ nên tồn tại $a_i \in R^*$ sao cho $a_i a_j = e$ hay a_i là phần tử nghịch đảo của a_j . Do đó R là một trường.

12. a) \Rightarrow b) Cho I là một idéan của R , $I \neq \{0\}$. Khi đó tồn tại $x \in I$, $x \neq 0$, do R là một trường nên x khả nghịch và ta có $1 = x \cdot x^{-1} \in I$. Do đó với mỗi $a \in R$, $a = a \cdot 1 \in I$, nên $I = R$.

b) \Rightarrow c) Cho f là một đồng cấu vành khác không từ R vào vành khác không S . Khi đó $\text{Ker } f$ là một idéan của R , nên $\text{Ker } f = \{0\}$ hoặc $\text{Ker } f = R$. Do $f \neq 0$ và $S \neq \{0\}$ nên $\text{Ker } f = \{0\}$ hay f là một đơn cấu.

c) \Rightarrow a) Với $x \in R$, $x \neq 0$, xét idéan $\langle x \rangle$ sinh ra bởi x , nghĩa là $\langle x \rangle = \{ax \mid a \in R\}$. Giả sử $\langle x \rangle \neq R$. Khi đó $R/\langle x \rangle$ là vành khác không và $p : R \rightarrow R/\langle x \rangle : a \mapsto a + \langle x \rangle$ là một đồng cấu vành khác không. Do đó p là một đơn cấu hay $\langle x \rangle = \text{Ker } p = \{0\}$. Điều vô lý này cho biết $\langle x \rangle = R$. Từ đó $1 \in \langle x \rangle$ hay tồn tại $a \in R$ sao cho $ax = 1$ hay x là khả nghịch. Vậy R là một trường.

13. Đặt $T = \left\{ \begin{pmatrix} a & b \\ 3b & a \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}$ thì T là một tập con khác rỗng của vành $M_2(\mathbb{Q})$ các ma trận vuông cấp 2 trên \mathbb{Q} với phép cộng và nhân ma trận và chứa ma trận đơn vị $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Ta có

$$\begin{aligned} \begin{pmatrix} a & b \\ 3b & a \end{pmatrix} - \begin{pmatrix} a' & b' \\ 3b' & a' \end{pmatrix} &= \begin{pmatrix} a - a' & b - b' \\ 3(b - b') & a - a' \end{pmatrix}, \\ \begin{pmatrix} a & b \\ 3b & a \end{pmatrix} \begin{pmatrix} a' & b' \\ 3b' & a' \end{pmatrix} &= \begin{pmatrix} aa' + 3bb' & ab' + ba' \\ 3(ba' + ab') & 3bb' + aa' \end{pmatrix}, \\ \begin{pmatrix} a & b \\ 3b & a \end{pmatrix} \begin{pmatrix} a' & b' \\ 3b' & a' \end{pmatrix} &= \begin{pmatrix} a' & b' \\ 3b' & a' \end{pmatrix} \begin{pmatrix} a & b \\ 3b & a \end{pmatrix} \end{aligned}$$

Vậy T là một vành con giao hoán của $M_2(\mathbb{Q})$ có chứa đơn vị của $M_2(\mathbb{Q})$. Do đó T là một vành giao hoán khác 0 có đơn vị. Ngoài ra, với $\begin{pmatrix} a & b \\ 3b & a \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ (khi đó $a^2 - 3b^2 \neq 0$), ta có

$$\begin{pmatrix} a & b \\ 3b & a \end{pmatrix} \begin{pmatrix} \frac{a}{a^2 - 3b^2} & \frac{-b}{a^2 - 3b^2} \\ \frac{-3b}{a^2 - 3b^2} & \frac{a}{a^2 - 3b^2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Do đó T là một trường.

Xét ánh xạ

$$f : T \longrightarrow A : \begin{pmatrix} a & b \\ 3b & a \end{pmatrix} \mapsto a + b\sqrt{3}.$$

Rõ ràng f là một toàn ánh. f còn là một đơn ánh vì với $a + b\sqrt{3} = a' + b'\sqrt{3}$ thì $a = a'$ và $b = b'$ tức là $\begin{pmatrix} a & b \\ 3b & a \end{pmatrix} = \begin{pmatrix} a' & b' \\ 3b' & a' \end{pmatrix}$. Ngoài ra,

$$\begin{aligned} f\left(\begin{pmatrix} a & b \\ 3b & a \end{pmatrix} + \begin{pmatrix} a' & b' \\ 3b' & a' \end{pmatrix}\right) &= f\left(\begin{pmatrix} a+a' & b+b' \\ 3(b+b') & a+a' \end{pmatrix}\right) \\ &= (a+a') + (b+b')\sqrt{3} = (a+b\sqrt{3}) + (a'+b'\sqrt{3}) \\ &= f\left(\begin{pmatrix} a & b \\ 3b & a \end{pmatrix}\right) + f\left(\begin{pmatrix} a' & b' \\ 3b' & a' \end{pmatrix}\right), \end{aligned}$$

$$\begin{aligned} f\left(\begin{pmatrix} a & b \\ 3b & a \end{pmatrix} \begin{pmatrix} a' & b' \\ 3b' & a' \end{pmatrix}\right) &= f\left(\begin{pmatrix} aa' + 3bb' & ab' + ba' \\ 3(ba' + ab') & 3bb' + aa' \end{pmatrix}\right) \\ &= (aa' + 3bb') + (ab' + ba')\sqrt{3} = (a+b\sqrt{3})(a'+b'\sqrt{3}) \\ &= f\left(\begin{pmatrix} a & b \\ 3b & a \end{pmatrix}\right)f\left(\begin{pmatrix} a' & b' \\ 3b' & a' \end{pmatrix}\right). \end{aligned}$$

Vậy f là một đẳng cấu.

14. Đặt $T = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$ thì T là một tập con khác rỗng của vành $M(2, \mathbb{R})$ các ma trận vuông cấp 2 trên \mathbb{R} với phép cộng và nhân ma trận và chứa ma trận đơn vị $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Ta có

$$\begin{aligned} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} - \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} &= \begin{pmatrix} a-a' & b-b' \\ -(b-b') & a-a' \end{pmatrix}, \\ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} &= \begin{pmatrix} aa' - bb' & ab' + ba' \\ -(ba' + ab') & -bb' + aa' \end{pmatrix}, \\ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} &= \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \end{aligned}$$

Vậy T là một vành con giao hoán của $M(2, \mathbb{R})$ có chứa đơn vị của $M(2, \mathbb{R})$. Do đó T là một vành giao hoán khác 0 có đơn vị. Ngoài ra, với $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ (khi đó $a^2 + b^2 \neq 0$), ta có

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} \frac{a}{a^2+b^2} & \frac{-b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Do đó T là một trường.

Xét ánh xạ

$$f : T \longrightarrow A : \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mapsto a + bi.$$

Rõ ràng f là một toàn ánh. f còn là một đơn ánh vì với $a + bi = a' + b'i$ thì $a = a'$ và $b = b'$ tức là $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix}$. Ngoài ra,

$$\begin{aligned} f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix}\right) &= f\left(\begin{pmatrix} a+a' & b+b' \\ -(b+b') & a+a' \end{pmatrix}\right) \\ &= (a+a') + (b+b')i = (a+bi) + (a'+b'i); \\ &= f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) + f\left(\begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix}\right), \end{aligned}$$

$$\begin{aligned} f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix}\right) &= f\left(\begin{pmatrix} aa' - bb' & ab' + ba' \\ -(ba' + ab') & -bb' + aa' \end{pmatrix}\right) \\ &= (aa' - bb') + (ab' + ba')i = (a+bi)(a'+b'i) \\ &= f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right)f\left(\begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix}\right). \end{aligned}$$

Vậy f là một đẳng cấu.

15. a) Ta có $\mathbb{Q}(\sqrt{p})$ là một tập con khác rỗng của trường \mathbb{R} các số thực và có chứa số nguyên 1 (vì $1 = 1 + 0\sqrt{p}$). $\forall a, b, a', b' \in Q$,

$$\begin{aligned} (a + b\sqrt{p}) - (a' + b'\sqrt{p}) &= (a - a') + (b - b')\sqrt{p}, \\ (a + b\sqrt{p})(a' + b'\sqrt{p}) &= (aa' + pbb') + (ab' + ba')\sqrt{p}. \end{aligned}$$

Vậy $\mathbb{Q}(\sqrt{p})$ là một vành con của \mathbb{R} chứa 1, nên nó là một vành giao hoán có đơn vị. Ngoài ra, với $a + b\sqrt{p} \in \mathbb{Q}(\sqrt{p})$ và khác 0 (a và b không

đồng thời bằng 0), ta có $a^2 - pb^2 \neq 0$, $\frac{a}{a^2 - pb^2} + \frac{-b}{a^2 - pb^2} \in \mathbb{Q}(\sqrt{p})$ và $(a + b\sqrt{p})(\frac{a}{a^2 - pb^2} + \frac{-b}{a^2 - pb^2}) = 1$. Do đó $\mathbb{Q}(\sqrt{p})$ là một trường.

b) Giả sử tồn tại đẳng cấu trường $f : \mathbb{Q}(\sqrt{7}) \rightarrow \mathbb{Q}(\sqrt{11})$. Khi đó $f(1) \neq 0$ và do $f(1) = f(1.1) = f(1)f(1)$ nên $f(1) = 1$. Từ đó $f(7) = f(7.1) = 7f(1) = 7$. Giả sử $f(\sqrt{7}) = a + b\sqrt{11}$ (với $a, b \in \mathbb{Q}$). Ta có

$$7 = f(7) = f(\sqrt{7} \cdot \sqrt{7}) = f(\sqrt{7})^2 = (a + b\sqrt{11})^2,$$

hay $a^2 + 11b^2 + 2ab\sqrt{11} = 7$ hay $2ab\sqrt{11} = 7 - a^2 - 11b^2$.

- Nếu $a = b = 0$ thì $0 = 7$: vô lý.

- Nếu $a = 0$ và $b \neq 0$ thì $b = \sqrt{\frac{7}{11}}$: vô lý.

- Nếu $b = 0$ và $a \neq 0$ thì $a = \sqrt{7}$: vô lý.

- Nếu $a \neq 0$ và $b \neq 0$ thì $\sqrt{11} = \frac{7-a^2-11b^2}{2ab}$: vô lý vì vé phải là một số hữu tỉ nhưng vé trái là một số vô tỉ.

16. Giả sử $f : \mathbb{F} \rightarrow \mathbb{F}$ là một tự đồng cấu của trường \mathbb{F} . Khi đó

$$f(1)(f(1) - 1) = f(1)f(1) - f(1) = f(1.1) - f(1) = 0,$$

do đó $f(1) = 0$ hay $f(1) = 1$.

- Nếu $f(1) = 0$ thì $f(a) = f(a.1) = f(a)f(1) = f(a).0 = 0$, $\forall a \in \mathbb{F}$, nên ta có $f = 0$.

- Nếu $f(1) = 1$ thì ta lần lượt xét \mathbb{F} là \mathbb{Q} , \mathbb{R} , \mathbb{Z}_p , \mathbb{C} . Ở đây, f là đơn cấu vì với $x \neq 0$, ta có $f(x)f(x^{-1}) = f(xx^{-1}) = f(1) = 1 \neq 0$ do đó $f(x) \neq 0$.

a) $\forall n \in \mathbb{Z}$, $f(n) = f(n.1) = nf(1) = n.1 = n$.

$\forall q \in \mathbb{Q}$, $q = \frac{n}{m}$, $n, m \in \mathbb{Z}$, $m \neq 0$, ta có $mf(q) = f(mq) = f(n) = n$, do đó $f(q) = \frac{n}{m} = q$.

Vậy các tự đồng cấu của trường \mathbb{Q} là ánh xạ 0 và ánh xạ đồng nhất.

b) Trước hết, nếu $r \in \mathbb{R}$, $r > 0$ thì $f(r) > 0$. Thật vậy, $f(r) = f(\sqrt{r} \cdot \sqrt{r}) = f(\sqrt{r})^2 > 0$ (vì nếu $f(\sqrt{r}) = 0$ thì do f đơn cấu ta có $\sqrt{r} = 0$ hay $r = 0$).

f là hàm tăng. Thật vậy, $\forall x, y \in \mathbb{R}$, $x < y$, ta có $y - x > 0$, nên $f(y) - f(x) = f(y - x) > 0$ hay $f(x) < f(y)$.

Giả sử $\exists z \in \mathbb{R}$ sao cho $f(z) \neq z$. Nếu $f(z) < z$ thì từ tính trừ mật của \mathbb{Q} trong \mathbb{R} tồn tại $q \in \mathbb{Q}$ sao cho $f(z) < q < z$. Khi đó

$q = f(q) < f(z)$, mâu thuẫn với $f(z) < q$. Tương tự, nếu $f(z) > z$ cũng dẫn đến mâu thuẫn. Do đó $f(z) = z, \forall z \in \mathbb{R}$.

Vậy các tự đồng cấu của trường \mathbb{R} là ánh xạ 0 và ánh xạ đồng nhất.

c) $\forall \bar{a} \in \mathbb{Z}_p, f(\bar{a}) = f(a \cdot \bar{1}) = af(\bar{1}) = a \cdot \bar{1} = \bar{a}$.

Vậy các tự đồng cấu của trường \mathbb{Z}_p là ánh xạ 0 và ánh xạ đồng nhất.

d) Giả sử $f : \mathbb{C} \rightarrow \mathbb{C}$ là một tự đồng cấu của trường số phức \mathbb{C} sao cho $f(a) = a$ với mọi $a \in \mathbb{R}$. Như vậy với số phức bất kỳ $z = a + ib \in \mathbb{C}$, ta có $f(z) = f(a + ib) = f(a) + f(b)f(i) = a + bf(i)$.

Vì $i^2 = -1$ nên $[f(i)]^2 = f(i^2) = f(-1) = -1$. Do đó $f(i) = i$ hoặc $f(i) = -i$. Vậy các tự đồng cấu của trường \mathbb{C} là ánh xạ đồng nhất và ánh xạ cho liên hợp ($z \mapsto \bar{z}$).

17. a) Rõ ràng $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in Q$. $\forall A = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}, A' = \begin{pmatrix} a' & b' \\ -\bar{b}' & \bar{a}' \end{pmatrix} \in Q$,

$$A - A' = \begin{pmatrix} a - a' & b - b' \\ -\bar{b} + \bar{b}' & \bar{a} - \bar{a}' \end{pmatrix} = \begin{pmatrix} a - a' & b - b' \\ -(\bar{b} - b') & \bar{a} - \bar{a}' \end{pmatrix} \in Q,$$

$$AA' = \begin{pmatrix} aa' - bb' & ab' + b\bar{a}' \\ -\bar{b}a' - \bar{a}\bar{b}' & -\bar{b}b' + \bar{a}\bar{a}' \end{pmatrix} = \begin{pmatrix} aa' - bb' & ab' + b\bar{a}' \\ -(ab' + b\bar{a}') & aa' - bb' \end{pmatrix} \in Q.$$

Cho $A = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, tức là $a\bar{a} + b\bar{b} > 0$. Khi đó A có nghịch đảo là $A^{-1} = \begin{pmatrix} \bar{a} & -b \\ \frac{a\bar{a} + b\bar{b}}{\bar{b}} & \frac{a\bar{a} + b\bar{b}}{a} \\ \frac{a\bar{a} + b\bar{b}}{a\bar{a} + b\bar{b}} & \frac{a\bar{a} + b\bar{b}}{a\bar{a} + b\bar{b}} \end{pmatrix} \in Q$

b) Dễ dàng kiểm tra được $I^2 = J^2 = K^2 = -1, IJ = -JI = K, JK = -KJ = I, KI = -IK = J$.

$\forall A = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \in Q$, đặt $a = a_1 + ia_2, b = b_1 + ib_2, a_1, a_2, b_1, b_2 \in \mathbb{R}$, ta có

$$\begin{aligned} A &= \begin{pmatrix} a_1 + ia_2 & b_1 + ib_2 \\ -b_1 + ib_2 & a_1 - ia_2 \end{pmatrix} \\ &= \begin{pmatrix} a_1 & 0 \\ 0 & a_1 \end{pmatrix} + \begin{pmatrix} ia_2 & 0 \\ 0 & -ia_2 \end{pmatrix} + \begin{pmatrix} 0 & b_1 \\ -b_1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & ib_2 \\ ib_2 & 0 \end{pmatrix} \\ &= a_1 + a_2 I + b_1 J + b_2 K. \end{aligned}$$

18. $xy = x(x^{-1} + y^{-1})y = y + x = -1.$

$$1 = (x+y)^2 = x^2 + 2xy + y^2 \Rightarrow x^2 + y^2 = 1 - 2xy = 3.$$

$$9 = (x^2 + y^2)^2 = x^4 + 2x^2y^2 + y^4 \Rightarrow x^4 + y^4 = 9 - 2(xy)^2 = 9 - 2 = 7.$$

19. Giả sử tồn tại một đẳng cấu nhóm $f : (K, +) \longrightarrow (K \setminus \{0\}, \cdot).$

1) $1 + 1 = 0$ (1 và 0 lần lượt là đơn vị và phần tử không ci)

$$\forall x \in K, x + x = x(1 + 1) = x \cdot 0 = 0,$$

$$(f(x))^2 = f(x + x) = f(0) = 1,$$

$$f(x) = 1 \text{ hoặc } f(x) = -1 = 1.$$

Như vậy $f(K) = \{1\}$, K hữu hạn. Điều này vô lý vì K và $K \setminus \{0\}$ không có cùng số phần tử.

2) $1 + 1 \neq 0.$

Ta ký hiệu $\alpha = f^{-1}(1)$, $\beta = f^{-1}(-1)$. Ta có

$$\begin{cases} f(2\alpha) = f(\alpha + \alpha) = (f(\alpha))^2 = 1^2 = 1, \\ f(2\beta) = f(\beta + \beta) = (f(\beta))^2 = (-1)^2 = 1. \end{cases}$$

Từ đó $2\alpha = 2\beta$ hay $(1+1)(\alpha - \beta) = 0$ vì f là song ánh. Điều này vô lý vì $1 + 1 \neq 0$ và $\alpha \neq \beta$.

20. I và J khác rỗng vì chứa ma trận không. Ta có

$$\begin{pmatrix} 0 & 0 & 0 \\ a & 0 & 0 \\ b & 2c & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 & 0 \\ a' & 0 & 0 \\ b' & 2c' & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ a - a' & 0 & 0 \\ b - b' & 2(c - c') & 0 \end{pmatrix},$$

$$\begin{pmatrix} x & 0 & 0 \\ y & z & 0 \\ t & u & v \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ a & 0 & 0 \\ b & 2c & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ za & 0 & 0 \\ ua + vb & 2vc & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 0 & 0 \\ a & 0 & 0 \\ b & 2c & 0 \end{pmatrix} \begin{pmatrix} x & 0 & 0 \\ y & z & 0 \\ t & u & v \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ ax & 0 & 0 \\ bx + 2cy & 2cz & 0 \end{pmatrix}.$$

Do đó I là một idéan hai phía của T .

$$\begin{pmatrix} 0 & 0 & 0 \\ l & 0 & 0 \\ 2m & 2n & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 & 0 \\ l' & 0 & 0 \\ 2m' & 2n' & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 0 & 0 \\ l - l' & 0 & 0 \\ 2(m - m') & 2(n - n') & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 0 & 0 \\ a & 0 & 0 \\ b & 2c & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ l & 0 & 0 \\ 2m & 2n & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 2cl & 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 0 & 0 \\ l & 0 & 0 \\ 2m & 2n & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ a & 0 & 0 \\ b & 2c & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 2na & 0 & 0 \end{pmatrix}.$$

Do đó J là một iđéan hai phía của I .

$$\begin{pmatrix} 0 & 0 & 0 \\ l & 0 & 0 \\ 2m & 2n & 0 \end{pmatrix} \begin{pmatrix} x & 0 & 0 \\ y & z & 0 \\ t & u & v \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ lx & 0 & 0 \\ 2(mx + ny) & 2nz & 0 \end{pmatrix},$$

$$\begin{pmatrix} x & 0 & 0 \\ y & z & 0 \\ t & 1 & v \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 2m & 2n & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ z & 0 & 0 \\ 1 + 2vm & 2vn & 0 \end{pmatrix}.$$

Do đó J là một iđéan phải của T nhưng không là một iđéan trái của T .

21. a) Ta chứng minh các iđéan của \mathbb{Z} là $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$ với $n \in \mathbb{N}$ tuỳ ý.

Cho I là một iđéan của \mathbb{Z} . Nếu $I = \{0\}$ thì $I = n\mathbb{Z}$ với $n = 0$. Nếu $I \neq \{0\}$ thì gọi n là số nguyên dương nhỏ nhất sao cho $n \in I$, ta có $I = n\mathbb{Z}$.

Đảo lại, với n là một số tự nhiên tuỳ ý thì kiểm tra được $n\mathbb{Z}$ là một iđéan của \mathbb{Z} .

b) Cho dãy tăng các iđéan của \mathbb{Z} :

$$I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$$

Khi đó tồn tại các số tự nhiên $k_1, k_2, \dots, k_n, \dots$ sao cho $I_j = k_j\mathbb{Z}$, với $j \geq 1$. Do $m\mathbb{Z} \subset n\mathbb{Z}$ khi và chỉ khi $n|m$, nên ta có $k_2|k_1, k_3|k_2, \dots, k_{n+1}|k_n, \dots$. Vì vậy, tồn tại i sao cho $k_i = k_{i+1} = k_{i+2} = \dots$, tức là $I_j = I_i, \forall j > i$.

Dãy giảm các iđéan của \mathbb{Z} :

$$p\mathbb{Z} \supset p^2\mathbb{Z} \supset \cdots \supset p^n\mathbb{Z} \supset \cdots$$

là không dừng.

22. Ta có các toàn cầu vành sau:

$$p_1 : R \times S \longrightarrow R : (x, y) \mapsto x, p_2 : R \times S \longrightarrow S : (x, y) \mapsto y.$$

Nếu I là một iđéan của R và J là một iđéan của S thì dễ dàng có được $I \times J$ là một iđéan của $R \times S$.

Cho M là một iđéan của vành tích $R \times S$. Đặt $I = p_1(M)$ và $J = p_2(M)$ thì I và J lần lượt là iđéan của R và S . $\forall (x, y) \in M, x = p_1(x, y) \in I, y = p_2(x, y) \in J$ nên $(x, y) \in I \times J$. Đảo lại, $\forall (x, y) \in I \times J, \exists x_1 \in R, y_1 \in S$ sao cho $(x, y_1), (x_1, y) \in M$; khi đó

$$(x, y) = (x, 0) + (0, y) = (1_R, 0)(x, y_1) + (0, 1_S)(x_1, y) \in M,$$

trong đó 1_R và 1_S lần lượt là đơn vị của R và S . Do đó $M = I \times J$.

Các iđéan của vành vành \mathbb{Z}^2 là $n\mathbb{Z} \times m\mathbb{Z}$ trong đó $n, m \in \mathbb{N}$. Các iđéan của vành \mathbb{R}^2 là $\{(0, 0)\}, \{0\} \times \mathbb{R}, \mathbb{R} \times \{0\}$ và $\mathbb{R} \times \mathbb{R}$.

23. a) Cho I là iđéan cực đại, giả sử $xy \in I$

$x \notin I \Rightarrow I + (x) = R \Rightarrow 1 = h + rx, h \in I, r \in R \Rightarrow y = hy + rxy \in I \Rightarrow I$ là iđéan nguyên tố.

b) Cho I là iđéan nguyên tố và J là iđéan sao cho $I \subsetneq J$. Khi đó

$\exists x \in J, x \notin I \Rightarrow \exists n > 1, x^n = x \Rightarrow x(x^{n-1} - 1) = 0 \in I \xrightarrow{x \notin I} z = x^{n-1} - 1 \in I \subset J \Rightarrow 1 = x^{n-1} - z \in J \Rightarrow J = R$.

Vậy I là iđéan cực đại.

24. a) Rõ ràng $\mathbb{Z}[i] \neq \emptyset$. $\forall a + ib, c + id \in \mathbb{Z}[i]$, ta có

$$(a + ib) - (c + id) = (a - c) + i(b - d) \in \mathbb{Z}[i],$$

$$(a + ib)(c + id) = (ac - bd) + i(ad + bc) \in \mathbb{Z}[i].$$

Do đó $\mathbb{Z}[i]$ là một vành con của \mathbb{C} .

Rõ ràng $\langle u \rangle \neq \emptyset$. $\forall ux, uy \in \langle u \rangle, \forall z \in \mathbb{Z}[i]$, ta có

$ux - uy = u(x - y) \in \langle u \rangle, z(ux) = u(zx) \in \langle u \rangle$. Vậy $\langle u \rangle$ là iđéan của $\mathbb{Z}[i]$.

b) $\mathbb{Z}[i]/\langle 2 \rangle$ có 4 phần tử $\bar{0}, \bar{1}, \bar{i}, \overline{1+i}$, trong đó, $\bar{x} = x + \langle 2 \rangle$, với $x \in \mathbb{Z}[i]$. Như vậy, $\overline{1+i} \neq \bar{0}$ và $\overline{1+i} \overline{1+i} = \overline{2i} = \bar{0}$. Do đó $\mathbb{Z}[i]/\langle 2 \rangle$ có ước của không, nên nó không là một trường.

c) $\mathbb{Z}[i]/\langle 3 \rangle$ có 9 phần tử $\alpha_0 = \bar{0}, \alpha_1 = \bar{1}, \alpha_2 = \bar{2}, \alpha_3 = \bar{i}, \alpha_4 = \overline{1+i}, \alpha_5 = \overline{2+i}, \alpha_6 = \overline{2i}, \alpha_7 = \overline{1+2i}, \alpha_8 = \overline{2+2i}$.

$\mathbb{Z}[i]/\langle 3 \rangle$ là vành giao hoán có đơn vị $\bar{1} = \alpha_1$. Ngoài ra,

$$\begin{aligned} \alpha_1^{-1} &= \alpha_1, \alpha_2^{-1} = \alpha_2, \alpha_3^{-1} = \alpha_6, \alpha_4^{-1} = \alpha_5, \\ \alpha_5^{-1} &= \alpha_4, \alpha_6^{-1} = \alpha_3, \alpha_7^{-1} = \alpha_8, \alpha_8^{-1} = \alpha_7. \end{aligned}$$

Vậy $\mathbb{Z}[i]/\langle 3 \rangle$ là một trường.

25. Rõ ràng

$$I = \{ra \mid r \in R\} \neq \emptyset \text{ và } J = \{ra + na \mid r \in R \text{ và } n \in \mathbb{Z}\} \neq \emptyset.$$

$$\forall r, s, t \in R, \forall n, m \in \mathbb{Z}, ra - sa = (r - s)a \in I,$$

$$t(ra) = (tr)a \in I,$$

$$(ra + na) - (sa + ma) = (r - s)a + (n - m)a \in J,$$

$$t(ra + na) = (tr + nt)a + 0a \in J.$$

Vậy $\{ra \mid r \in R\}$ và $\{ra + na \mid r \in R \text{ và } n \in \mathbb{Z}\}$ là các iđêan của R .

Nếu R có đơn vị 1 thì $a = 1a \in J = \{ra \mid r \in R\}$. Giả sử J là một iđêan của R chứa a . Khi đó $ra \in J, \forall r \in R$ hay $\{ra \mid r \in R\} \subset J$. Do đó $\{ra \mid r \in R\}$ là iđêan nhỏ nhất của R chứa a . Vậy $I = \{ra \mid r \in R\}$.

Nếu R không có đơn vị thì ta có $a = 0a + 1a \in \{ra + na \mid r \in R \text{ và } n \in \mathbb{Z}\}$. Giả sử K là một iđêan của R chứa a . Khi đó $ra + na \in K, \forall r \in R, \forall n \in \mathbb{Z}$. Khi đó $\{ra + na \mid r \in R \text{ và } n \in \mathbb{Z}\} \subset K$. Do đó $\{ra + na \mid r \in R \text{ và } n \in \mathbb{Z}\}$ là iđêan nhỏ nhất của R chứa a . Vậy $I = \{ra + na \mid r \in R \text{ và } n \in \mathbb{Z}\}$.

26. a) Rõ ràng $M(2, \mathbb{F}) \neq \emptyset$. Ký hiệu

$$I = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in M(2, \mathbb{F}) \mid a, b \in \mathbb{F} \right\}.$$

$$\text{Với mọi } \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} a' & b' \\ 0 & 0 \end{pmatrix} \in I, \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in M(2, \mathbb{F}),$$

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} a' & b' \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a - a' & b - b' \\ 0 & 0 \end{pmatrix} \in I,$$

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x & y \\ z & t \end{pmatrix} = \begin{pmatrix} ax + bz & ay + bt \\ 0 & 0 \end{pmatrix} \in I,$$

$$\begin{pmatrix} x & y \\ z & t \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} xa & xb \\ za & zb \end{pmatrix} \notin I \text{ khi } z \neq 0 \text{ và } a \neq 0.$$

Vậy I là 1 iđêan phải mà không là iđêan trái của $M(2, \mathbb{F})$.

b) Cho I là iđêan khác không của $M(2, \mathbb{Z}_2)$. Lấy $A = (a_{ij}) \in I, A \neq 0$, nên tồn tại $a_{rs} \neq 0$. Gọi $I_{ij} \in M(2, \mathbb{Z}_2)$ là ma trận mà phần tử dòng i , cột j bằng 1 và các phần tử còn lại bằng 0. Ta có

$$I_{sr} \cdot A \cdot I_{ss} = I_{ss},$$

vì $A \in I$ nên $I_{ss} \in I$. Với mỗi $i = 1, 2$, $I_{is}I_{ss}I_{si} = I_{ii}$ và do $I_{ss} \in I$ nên $I_{ii} \in I$, với mọi $i = 1, 2$. Từ đó ma trận đơn vị $I_2 = I_{11} + I_{22} \in I$ và điều này dẫn đến $I = M(2, \mathbb{Z}_2)$.

27. Lấy $a \in R \setminus \{0\}$. Nhóm con I của nhóm cộng R sinh bởi a là một idéan của R . Do đó với mỗi $x \in \mathbb{N}$ tồn tại $z_x \in \mathbb{Z}$ sao cho $ax = z_x a$.

* $\forall m \in \mathbb{Z} \setminus \{0\}$, $ma \neq 0$: $\forall x, y \in R$, $\exists z_x, z_y \in \mathbb{Z}$, $ax = z_x a$, $ay = z_y a$; khi đó, $x = y \Leftrightarrow ax = ay \Leftrightarrow z_x a = z_y a \Leftrightarrow (z_x - z_y)a = 0 \Leftrightarrow z_x - z_y = 0 \Leftrightarrow z_x = z_y$; do đó ánh xạ

$$f : R \longrightarrow \mathbb{Z} : x \mapsto z_x$$

là một đơn ánh. Ngoài ra, do $a(x+y) = ax+ay = (z_x+z_y)a$ và $a(xy) = (ax)y = (z_x a)y = z_x(ay) = z_x(z_y a) = (z_x z_y)a$ nên $f(x+y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$. Vậy f là một đơn cấu vành hay R đẳng cấu với vành con $f(R)$ của vành \mathbb{Z} .

* $\exists m \in \mathbb{Z} \setminus \{0\}$, $ma = 0$: Gọi p là số nguyên dương nhỏ nhất sao cho $pa = 0$. Nếu $p = qr$ với $1 < q, r < p$ thì $qa.ra = qra^2 = pa.a = 0$ nên $qa = 0$ hay $ra = 0$ (do R không có ước của không). Điều này dẫn đến mâu thuẫn với tính nhỏ nhất của p . Vậy p là một số nguyên tố. $\forall x, y \in R$, $\exists z_x, z_y \in \mathbb{Z}$, $ax = z_x a$, $ay = z_y a$; khi đó, $x = y \Leftrightarrow ax = ay \Leftrightarrow z_x a = z_y a \Leftrightarrow (z_x - z_y)a = 0 \Leftrightarrow p|(z_x - z_y) \Leftrightarrow \overline{z_x} = \overline{z_y}$ (trong \mathbb{Z}_p); do đó ánh xạ

$$f : R \longrightarrow \mathbb{Z}_p : x \mapsto \overline{z_x}$$

là một đơn ánh. Do $\overline{z_x + z_y} = \overline{z_x} + \overline{z_y}$, $\overline{z_x z_y} = \overline{z_x} \overline{z_y}$ nên f là một đơn cấu vành. Vì $f \neq 0$ nên $f(R) = \mathbb{Z}_p$ hay f còn là một toàn cấu. Vậy f là một đẳng cấu vành.

28. a) Ma trận A là ước bên trái của không trong vành \mathcal{M} khi và chỉ khi tồn tại $B \in \mathcal{M}$ sao cho $B \neq 0$ và $AB = 0$, tức là khi và chỉ khi tồn tại $X \in \mathbb{R}^n$ sao cho $X \neq 0$ và $AX = 0$ (chính là một cột của B). Điều này tương đương với $\det(A) = 0$. Tương tự cho ước bên phải của không bằng cách thay cột bởi dòng.

b) Rõ ràng $\mathcal{N} \neq \emptyset$; ngoài ra,

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix} - \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

$$\begin{aligned}
 &= \begin{pmatrix} a_{11} - b_{11} & a_{12} - b_{12} & \dots & a_{1n} - b_{1n} \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}, \\
 &\quad \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix} \\
 &= \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & \dots & a_{11}b_{1n} \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}.
 \end{aligned}$$

Do đó \mathcal{N} là một vành con của \mathcal{M} và mọi ma trận khác không của \mathcal{N} đều là ước bên phải của không trong vành \mathcal{N} . Thật vậy, trong tích 2 ma trận ở trên, chọn $a_{11} = 0$ và a_{12}, \dots, a_{1n} không đồng thời bằng 0 thì tích này bằng ma trận không. Ma trận trong \mathcal{N} mà phần tử dòng 1 cột 1 khác 0 ($a_{11} \neq 0$) đều không phải là ước bên trái của không trong vành \mathcal{N} .

c) Các đơn vị trái trong \mathcal{N} là các ma trận có phần tử dòng 1 cột 1 bằng 1 và các phần tử khác của dòng 1 là tùy ý.

29. a) Mỗi đồng cấu nhóm cộng $f : \mathbb{Z}_m \rightarrow \mathbb{Z}_n$ xác định giá trị $a = f(\bar{1}) \in \mathbb{Z}_n$ và do $m\bar{a} = mf(\bar{1}) = f(m\bar{1}) = f(\bar{m}) = f(\bar{0}) = \bar{0}$ nên ta có cấp của a trong \mathbb{Z}_n là một ước của m (do đó là một ước chung của m và n). Đảo lại, phần tử $a \in \mathbb{Z}_n$ có cấp là một ước của m thì phép tương ứng $f : \mathbb{Z}_m \rightarrow \mathbb{Z}_n : \bar{k} \mapsto ka$ là một ánh xạ và khi đó f là một đồng cấu nhóm cộng.

$(72, 30) = 6$ và các phần tử của \mathbb{Z}_{42} có cấp ước của 6 là:

$$\bar{0}, \bar{5}, \bar{10}, \bar{15}, \bar{20}, \bar{25}.$$

Do đó các đồng cấu nhóm cộng từ \mathbb{Z}_{72} vào \mathbb{Z}_{30} là:

$$f_0(\bar{1}) = \bar{0}, f_1(\bar{1}) = \bar{5}, f_2(\bar{1}) = \bar{10}, f_3(\bar{1}) = \bar{15}, f_4(\bar{1}) = \bar{20}, f_5(\bar{1}) = \bar{25}.$$

Đồng cấu nhóm cộng $f : \mathbb{Z}_{72} \rightarrow \mathbb{Z}_{30}$ là đồng cấu vành $\Leftrightarrow \forall \bar{x}, \bar{y} \in \mathbb{Z}_{72}, f(\bar{x}\bar{y}) = f(\bar{x})f(\bar{y}) \Leftrightarrow f(\bar{1})^2 = f(\bar{1})$. Vậy tất cả các đồng cấu vành từ \mathbb{Z}_{72} vào \mathbb{Z}_{30} là:

$$f_0(\bar{k}) = \bar{0}, f_2(\bar{k}) = \bar{10k}, f_3(\bar{k}) = \bar{15k}, f_5(\bar{k}) = \bar{25k}.$$

b) $\text{Im } f_0 = 0\mathbb{Z}_{30} = \{0\}$, $\text{Ker } f_0 = \mathbb{Z}_{72}$.

$\text{Im } f_2 = 10\mathbb{Z}_{30} = \{\bar{0}, \bar{10}, \bar{20}\}$, $\text{Ker } f_2 = 3\mathbb{Z}_{72}$,

$\text{Im } f_3 = 15\mathbb{Z}_{30} = \{\bar{0}, \bar{15}\}$, $\text{Ker } f_3 = 2\mathbb{Z}_{72}$,

$\text{Im } f_5 = 25\mathbb{Z}_{30} = \{\bar{0}, \bar{25}, \bar{20}, \bar{15}, \bar{10}, \bar{35}\}$, $\text{Ker } f_5 = 6\mathbb{Z}_{72}$.

30. a) $\forall r, r' \in R$, $\phi(r + r') = (r + r' + I, r + r' + J) = (r + I, r + J) + (r' + I, r' + J) = \phi(r) + \phi(r')$ và $\phi(rr') = (rr' + I, rr' + J) = ((r+I)(r'+I), (r+J)(r'+J)) = (r+I, r+J)(r'+I, r'+J) = \phi(r)\phi(r')$. Do đó ϕ là một đồng cấu vành.

$r \in \text{Ker } \phi \Leftrightarrow \phi(r) = (r + I, r + J) = (I, J) \Leftrightarrow r + I = I$ và $r + J = J \Leftrightarrow r \in I$ và $r \in J \Leftrightarrow r \in I \cap J$. Do đó $\text{Ker } \phi = I \cap J$.

b) Do $I + J = R$, tồn tại $a \in I$, $b \in J$ sao cho $a + b = 1$.

$\forall (s + I, t + J) \in R/I \times R/J$, $\exists r = sb + ta$ (ở đây $s = sa + sb$ và $t = ta + tb$) sao cho $r - s = ta - sa = (t - s)a \in I$ và $r - t = (s - t)b \in J$, tức là $\phi(r) = (r + I, r + J) = (s + I, t + J)$. Do đó ϕ là một toàn cầu vành.

Vì $IJ \subset I$ và $IJ \subset J$ nên $IJ \subset I \cap J$. Với mọi $r \in I \cap J$, $r = ar + br \in IJ$ hay $I \cap J \subset IJ$. Vậy $I \cap J = IJ$.

ϕ là một toàn cầu và $\text{Ker } \phi = IJ$, nên ta có đẳng cầu:

$$R/IJ \cong R/I \times R/J.$$

31. a) Do $[x^3 + x] = [0]$ nên $[x^3] = -[x] = [x]$, $[x^4] = [x^2]$.

$$\mathbb{Z}_2[x]/(x^3 + x) = \{[0], [1], [x], [x+1], [x^2], [x^2+1], [x^2+x], [x^2+x+1]\}.$$

.	[0]	[1]	[x]	[x+1]	[x^2]	[x^2+1]	[x^2+x]	[x^2+x+1]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[x]	[x+1]	[x^2]	[x^2+1]	[x^2+x]	[x^2+x+1]
[x]	[0]	[x]	[x^2]	[x^2+x]	[x]	[0]	[x^2+x]	[x^2]
[x+1]	[0]	[x+1]	[x^2+x]	[x^2+1]	[x^2+x]	[x^2+1]	[0]	[x+1]
[x^2]	[0]	[x^2]	[x]	[x^2+x]	[x^2]	[0]	[x^2+x]	[x]
[x^2+1]	[0]	[x^2+1]	[0]	[x^2+1]	[0]	[x^2+1]	[0]	[x^2+1]
[x^2+x]	[0]	[x^2+x]	[x^2+x]	[0]	[x^2+x]	[0]	[0]	[x^2+x]
[x^2+x+1]	[0]	[x^2+x]	[x^2]	[x+1]	[x]	[x^2+1]	[x^2+x]	[0]
+1]		+1]						

b) Do $[x][x^2 + 1] = [0]$, $[x + 1][x^2 + x] = [0]$, $[x^2][x^2 + 1] = [0]$ và $[x^2 + x + 1]^2 = 1$, S chỉ có hai phần tử khá nghịch là $[1]$ và $[x^2 + x + 1]$.

32. $x^2 - x + 1$ là một đa thức bậc hai có $\Delta = -3 < 0$ nên không có nghiệm trong \mathbb{R} , do đó nó bất khả quy trong $\mathbb{R}[x]$.

Vành $\mathbb{R}[x]$ là miền nguyên các iđéan chính, nghĩa là nếu I là một iđéan của $\mathbb{R}[x]$ thì I sinh ra bởi một đa thức $f(x) \in \mathbb{R}[x]$ nào đó.

Cho $p(x)$ là một đa thức bất khả quy trong $\mathbb{R}[x]$ và $\mathcal{T}[\bar{\alpha}]$ một iđéan của $\mathbb{R}[x]$ sao cho $(p(x)) \subsetneq J \subset \mathbb{R}[x]$. Khi đó

$$J = (g(x)) \text{ với } g(x) \in \mathbb{R}[x], g(x) \neq 0, g(x)|p(x).$$

Do $p(x)$ bất khả quy nên $g(x) = c$ (hằng số khác 0), suy ra $1 = \frac{1}{c} \cdot c \in J$ hay $J = \mathbb{R}[x]$. Vậy $(p(x))$ là iđéan cực đại.

33. Ánh xạ $\varphi : \mathbb{Z}[x] \rightarrow \mathbb{Z}_7$ được định nghĩa như sau:

Với $f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{Z}[x]$, chia $f(x)$ cho $x - 5$, ta có $f(x) = (x - 5)g(x) + a_f$, $g(x) \in \mathbb{Z}[x]$, $a_f \in \mathbb{Z}$,

$$\varphi(f(x)) = \overline{a_f}.$$

Rõ ràng φ là một toàn ánh. Với $f_1(x) = (x - 5)g_1(x) + a_{f_1}$, $g_1(x) \in \mathbb{Z}[x]$, $a_{f_1} \in \mathbb{Z}$, ta có:

$$f(x) + f_1(x) = (x - 5)(g(x) + g_1(x)) + a_f + a_{f_1},$$

$$f(x)f_1(x) = (x - 5)((x - 5)g(x)g_1(x) + a_{f_1}g(x) + a_fg_1(x)) + a_fa_{f_1},$$

$$\varphi(f(x) + f_1(x)) = \overline{a_f + a_{f_1}} = \overline{a_f} + \overline{a_{f_1}} = \varphi(f(x)) + \varphi(f_1(x)),$$

$$\varphi(f(x)f_1(x)) = \overline{a_f a_{f_1}} = \overline{a_f} \overline{a_{f_1}} = \varphi(f(x))\varphi(f_1(x)).$$

Do đó φ là một toàn cầu.

$$f(x) = (x - 5)g(x) + a_f \in \text{Ker}\varphi, g(x) \in \mathbb{Z}[x], a_f \in \mathbb{Z}$$

$$\Rightarrow \overline{a_f} = \varphi(f(x)) = \overline{0} \Rightarrow a_f = 7k, \text{ với } k \in \mathbb{Z}$$

$$\Rightarrow f(x) = (x - 5)g(x) + 7k \in I.$$

$$f(x) = (x - 5)g(x) + 7h(x) \in I$$

$$\Rightarrow f(x) = (x - 5)g(x) + 7((x - 5)k(x) + a_h) \Rightarrow \varphi(f(x)) = \overline{7a_h} = \overline{0}$$

$$\Rightarrow f(x) \in \text{Ker}\varphi.$$

Do đó $\text{Ker}\varphi = I$. Vậy $\mathbb{Z}[x]/\text{Ker}\varphi \cong \text{Im}\varphi$ hay $\mathbb{Z}[x]/I \cong \mathbb{Z}_7$.

34. Ta có $a^4 = -1$. Do $0 = 0 + 0.a + 0.a^2 + 0.a^3 \in S$ nên $S \neq \emptyset$.

$\forall m, n, p, q, m', n', p', q' \in \mathbb{Z}$,

$$(m + na + pa^2 + qa^3) - (m' + n'a + p'a^2 + q'a^3) \\ = (m - m') + (n - n')a + (p - p')a^2 + (q - q')a^3 \in S,$$

$$(m + na + pa^2 + qa^3)(m' + n'a + p'a^2 + q'a^3) \\ = ((m - m') - nq' - qn' - pp') + (mn' + nm' - pq' - qp')a \\ + (mp' + pm' + nn' - qq')a^2 + (mq' + qm' + np' + pn')a^3 \in S$$

và $a = 0 + 1.a + 0.a^2 + 0.a^3 \in S$.

Do đó S là một vành con của \mathbb{C} chứa a .

Giả sử T là một vành con của \mathbb{C} chứa a . Khi đó $\forall m, n, p, q \in \mathbb{Z}$, $m = (-m)a^4, na, pa^2, qa^3 \in T$ nên $m + na + pa^2 + qa^3 \in T$. Do đó $S \subset T$. Vậy S là vành con nhỏ nhất của \mathbb{C} chứa a hay S là vành con sinh bởi a .

S không là một iđêan của \mathbb{C} vì với $i\frac{\sqrt{2}}{2} \in \mathbb{C}$, $1 \in S$, đẳng thức

$$i\frac{\sqrt{2}}{2} = i\frac{\sqrt{2}}{2} \cdot 1 = m + na + pa^2 + qa^3 \\ = \left(m + \frac{n\sqrt{2}}{2} - \frac{q\sqrt{2}}{2}\right) + \left(\frac{n\sqrt{2}}{2} + \frac{q\sqrt{2}}{2} + p\right)i$$

không xảy ra với mọi $m, n, p, q \in \mathbb{Z}$, vì khi đó $m = n - q = p = 0$, $n + q = 1$ và suy ra $n = q = \frac{1}{2}$.

35. a) Nếu $n = rs$, trong đó $0 < r, s < n$ thì $0 = n \cdot 1 = (rs) \cdot 1 = (r \cdot 1)(s \cdot 1)$ và do D là một miền nguyên nên suy ra $r \cdot 1 = 0$ hoặc $s \cdot 1 = 0$. Điều này vô lý vì n là cấp của 1. Do đó n là một số nguyên tố.

b) Do n là một số nguyên tố nên các hệ số nhị thức Newton $C_n^i = \frac{n!}{i!(n-i)!}$ là bội số của n với mọi i thoả mãn $0 < i < n$. Do đó với $0 < i < n$, ta có $C_n^i = kn$ ($k \in \mathbb{Z}$) và $C_n^i \cdot a = (kn) \cdot a = (k \cdot 1)(n \cdot a) = 0$, $\forall a \in D$. Từ đó vì D giao hoán, ta có:

$$\begin{aligned} \varphi(x+y) &= (x+y)^n = \sum_{i=0}^n C_n^i x^i y^{n-i} = x^n + y^n + \sum_{i=1}^{n-1} C_n^i x^i y^{n-i} \\ &= x^n + y^n = \varphi(x) + \varphi(y), \\ \varphi(xy) &= (xy)^n = x^n y^n = \varphi(x)\varphi(y). \end{aligned}$$

Vậy φ là một đồng cấu vành.

BÀI TẬP CHƯƠNG III – VÀNH ĐA THỨC

1. Tìm tất cả các đa thức hệ số thực $P(x)$ thoả mãn điều kiện $P(0) = 0$ và đồng nhất thức:

$$P(x) = \frac{1}{2}(P(x+1) + P(x-1)) \quad \forall x \in \mathbb{R}.$$

2. a) Cho $f(x)$ là đa thức bậc n với hệ số thực và $f'(x)$ là đạo hàm của $f(x)$. Biết rằng $f(x)$ có n nghiệm thực x_1, x_2, \dots, x_n . Chứng minh rằng nếu số thực a không phải là nghiệm của $f(x)$ thì

$$\frac{1}{a-x_1} + \frac{1}{a-x_2} + \cdots + \frac{1}{a-x_n} = \frac{f'(a)}{f(a)}.$$

- b) Cho đa thức $\varphi(x) = x^3 + x^2 - 4x + 1$ có 3 nghiệm thực x_1, x_2, x_3 .
Tính

$$A = \frac{1}{x_1^2 - 3x_1 + 2} + \frac{1}{x_2^2 - 3x_2 + 2} + \frac{1}{x_3^2 - 3x_3 + 2},$$

$$B = \frac{1}{x_1^2 - 2x_1 + 1} + \frac{1}{x_2^2 - 2x_2 + 1} + \frac{1}{x_3^2 - 2x_3 + 1}.$$

3. Chứng minh rằng với mọi số tự nhiên n , đa thức

$$(x+1)^{2n+1} + x^{n+2}$$

chia hết cho đa thức $x^2 + x + 1$.

4. Cho k và n là hai số nguyên dương, r là dư của phép chia Euclid k cho n . Chứng minh rằng dư của phép chia Euclid x^k cho $x^n - 1$ là x^r .

5. Cho n là một số nguyên dương và φ là một số thực. Tìm dư của phép chia Euclid $(x \sin \varphi + \cos \varphi)^n$ cho $x^2 + 1$ trong $\mathbb{C}[x]$.

6. Trên trường \mathbb{Q} các số hữu tỉ, tìm ước chung lớn nhất của

$$f(x) = 2x^4 - x^3 + x^2 + 3x + 1, \quad g(x) = 2x^3 - 3x^2 + 2x + 2$$

và sau đó biểu thị nó như là tổ hợp tuyến tính của các đa thức đã cho.

7. Trên trường \mathbb{Z}_3 , tìm ước chung lớn nhất của

$$f(x) = x^5 + x^3 + x^2 + x + \bar{1}, \quad g(x) = x^3 + \bar{2}x^2 + x + \bar{1}.$$

8. Cho A, B, C thuộc $F[x]$, F là một trường. Chứng minh rằng nếu A, B, C nguyên tố cùng nhau từng đôi một thì $AB + BC + CA$ và ABC nguyên tố cùng nhau.

9. Chứng minh rằng trong $\mathbb{R}[x]$ các đa thức $A = x^4 + 1$ và $B = x^3 - 1$ nguyên tố cùng nhau và tìm một cặp $U, V \in \mathbb{R}[x]$ thoả mãn:

$$AU + BV = 1.$$

10. Dùng tiêu chuẩn Eisenstein để chứng minh các đa thức sau là bất khả quy trong $\mathbb{Q}[x]$:

- a) $x^4 - 13x^3 + 45x^2 - 61x + 25$.
- b) $x^4 + x^3 + x^2 + x + 1$.

11. a) Dùng tiêu chuẩn Eisenstein để chứng minh đa thức sau là bất khả quy trong $\mathbb{Q}[x]$:

$$x^3 - 3x + 1.$$

b) Trong vành $\mathbb{Q}[x]$, chứng minh rằng đa thức $f(x) = x^3 - 3n^2x + n^3$ với n là một số nguyên dương, là một đa thức bất khả quy.

12. Cho n là một số nguyên dương, a và b là hai số thực khác nhau. Tìm hai đa thức U và V trong $\mathbb{R}[x]$ sao cho

$$\begin{cases} U(x-a)^n + V(x-b)^n = 1, \\ \deg(U) \leq n-1, \deg(V) \leq n-1. \end{cases}$$

13. Tìm điều kiện cần và đủ để đa thức $f(x) = x^4 + px^2 + q \in \mathbb{Q}[x]$ là bất khả quy trên \mathbb{Q} .

14. Giả sử $f(x) = (x - a_1)(x - a_2) \dots (x - a_n) - 1$ với a_i là những số nguyên phân biệt, $i = 1, \dots, n$. Chứng minh rằng $f(x)$ là bất khả quy trên \mathbb{Q} .

15. Cho $P, Q, R \in \mathbb{C}[x]$ sao cho $P(x^3) + xQ(x^3) = (1 + x + x^2)R(x)$. Chứng minh rằng $x - 1$ chia hết P, Q, R .

16. Cho đa thức $A(x) = x^3 + x - 2$ với α, β là các nghiệm khác 1 của $A(x)$ trong \mathbb{C} .

- a) Tìm đa thức bậc hai $B(x) \in \mathbb{Q}[x]$ sao cho $B(1) = 1$, $B(\alpha) = \beta$, $B(\beta) = \alpha$.
- b) Chứng minh rằng $A(x)$ chia hết $B(B(x)) - x$.

17. Cho $n \in \mathbb{N}$ sao cho $n \geq 3$, $a_0, \dots, a_{n-3} \in \mathbb{R}$, $P = x^n + x^{n-1} + x^{n-2} + \sum_{k=0}^{n-3} a_k x^k$. Chứng minh rằng các nghiệm của P không phải đều là số thực.

18. Tìm tất cả các đa thức $P \in \mathbb{R}[x]$ sao cho:

$$P(0) = 1, P(1) = 0, P'(0) = 0, P'(1) = 1.$$

19. Trên trường \mathbb{R} các số thực, hãy phân tích phân thức hữu tỉ sau thành tổng các phân thức đơn giản:

$$\frac{-x^5 + 2x^4 - 4x^3 + 5x^2 - 4x + 3}{(x^2 + 1)^3}.$$

20. Trên trường \mathbb{Z}_7 các số nguyên modulo 7, hãy phân tích phân thức hữu tỉ sau thành tổng các phân thức đơn giản:

$$\frac{\bar{2}x^5 + \bar{3}x^3 + \bar{6}x^2 + \bar{3}}{(x^2 + \bar{1})^2}.$$

21. Trên trường \mathbb{Z}_5 các số nguyên modulo 5, hãy phân tích phân thức hữu tỉ sau thành tổng các phân thức đơn giản:

$$\frac{\bar{2}x^5 + \bar{3}x^3 + x^2 + \bar{1}}{(x^2 + \bar{1})^2}.$$

22. Cho đa thức $f(x) = (1 - x^2)^3 + 8x^3$.

- a) Tìm các nghiệm phức của đa thức $f(x)$.
- b) Phân tích đa thức $f(x)$ thành tích các đa thức bất khả quy hệ số thực.

23. Cho n là một số nguyên dương và hai đa thức

$$A = x^5 + 1, P_n = (x^4 - 1)(x^3 - x^2 + x - 1)^n + (x + 1)x^{4n-1} \in \mathbb{C}[x].$$

Chứng minh rằng A chia hết P_n .

24. Cho n là một số nguyên dương, $a, b \in \mathbb{C}$ sao cho $a \neq b$ và hai đa thức

$$A = (x - a)^{2n} + (x - b)^{2n}, B = (x - a)^2(x - b)^2 \in \mathbb{C}[x].$$

Xác định dư của phép chia Euclid A cho B .

25. Chứng minh rằng với mọi $n, p \in \mathbb{N}^*$, đa thức $\sum_{i=0}^{n-1} x^i$ chia hết đa thức $\left(\sum_{i=0}^n x^i\right)^p - x^n$ trong $\mathbb{F}[x]$ (\mathbb{F} là một trường tùy ý).

26. Với $n \in \mathbb{N}$, tính dư của phép chia Euclide $x^{2n+1} + (x+1)^{n+2}$ cho $x^2 + x + 1$ trong $\mathbb{C}[x]$.

27. Tìm điều kiện cần và đủ đối với $n \in \mathbb{N}^*$ để $x^2 + x + 1$ chia hết $(x^n + 1)^n - x^n$.

28. Cho hai đa thức $A, B \in \mathbb{F}[x] \setminus \{0\}$, với \mathbb{F} là một trường. Chứng minh rằng hai điều sau là tương đương:

a) A và B không nguyên tố cùng nhau.

b) Tồn tại $U, V \in \mathbb{F}[x] \setminus \{0\}$ sao cho $\deg(U) < \deg(B)$, $\deg(V) < \deg(A)$ và $AU + BV = 0$.

29. Cho $n \in \mathbb{N}^*$, a_0, \dots, a_{n-1} là các số thực không âm không đồng thời bằng 0 và $P = x^n - \sum_{k=0}^{n-1} a_k x^k$. Chứng minh rằng P có một và chỉ một nghiệm thực dương.

30. Cho $f(x)$ là một đa thức hệ số hữu tỉ có $\deg(f(x)) \geq 1$. Chứng minh rằng tồn tại đa thức hệ số hữu tỉ $g(x)$ sao cho

$$f(x)g(x) = a_2 x^2 + a_3 x^3 + a_5 x^5 + \cdots + a_p x^p,$$

với các lũy thừa với số mũ nguyên tố.

31. Cho $n \in \mathbb{N} \setminus \{0, 1\}$ và

$$P_n = x^{2n} - n^2 x^{n+1} + 2(n^2 - 1)x^n - n^2 x^{n-1} + 1 \in \mathbb{C}[x].$$

Chứng minh rằng 1 là nghiệm của P_n và xác định cấp bội của nó.

32. Cho $a, b, c \in \mathbb{Z}$ đôi một khác nhau và $P \in \mathbb{Z}[x]$. Chứng minh rằng ta không thể có

$$P(a) = b, P(b) = c, P(c) = a.$$

TRẢ LỜI VÀ HƯỚNG DẪN GIẢI BÀI TẬP
CHƯƠNG III – VÀNH ĐA THỨC

1. Rõ ràng $P(0) = 0P(1)$. Giả sử $P(k) = kP(1)$ với $0 \leq k \leq n$. Khi đó $P(n+1) = 2P(n) - P(n-1) = 2nP(1) - (n-1)P(1) = (n+1)P(1)$. Vậy theo nguyên lý quy nạp ta có $P(n) = nP(1)$, $\forall n \in \mathbb{N}$.

Do đó đa thức $xP(x) - xP(1)$ có vô số nghiệm, nên $P(x) - xP(1)$ là đa thức không. Đặt $a = P(1)$, ta có

$$P(x) = ax.$$

2. a) Ta có $f(x) = c(x - x_1)(x - x_2)\dots(x - x_n)$ với $c \in \mathbb{R}$, $c \neq 0$. Khi đó

$$(x) = c[(x - x_2)(x - x_3)\dots(x - x_n) + (x - x_1)(x - x_3)\dots(x - x_n) + \dots + (x - x_1)(x - x_2)\dots(x - x_{n-1})].$$

Từ đây suy ra

$$\frac{f'(a)}{f(a)} = \frac{1}{a - x_1} + \frac{1}{a - x_2} + \dots + \frac{1}{a - x_n}.$$

b)

$$\begin{aligned} A &= \frac{1}{(2-x_1)(1-x_1)} + \frac{1}{(2-x_2)(1-x_2)} + \frac{1}{(2-x_3)(1-x_3)} \\ &= \left(\frac{1}{1-x_1} + \frac{1}{1-x_2} + \frac{1}{1-x_3}\right) - \left(\frac{1}{2-x_1} + \frac{1}{2-x_2} + \frac{1}{2-x_3}\right) \\ &= \frac{\varphi'(1)}{\varphi(1)} - \frac{\varphi'(2)}{\varphi(2)}. \end{aligned}$$

Ta có $\varphi(1) = -1$, $\varphi(2) = 5$, $\varphi'(1) = 1$, $\varphi'(2) = 12$. Vậy $A = -\frac{17}{5}$.

Lấy đạo hàm 2 vé của $\frac{1}{x-x_1} + \frac{1}{x-x_2} + \frac{1}{x-x_3} = \frac{\varphi'(x)}{\varphi(x)}$, ta có

$$-\left(\frac{1}{(x-x_1)^2} + \frac{1}{(x-x_2)^2} + \frac{1}{(x-x_3)^2}\right) = \frac{\varphi(x)\varphi''(x) - \varphi'(x)^2}{\varphi(x)^2}.$$

Do đó $B = \frac{1}{(1-x_1)^2} + \frac{1}{(1-x_2)^2} + \frac{1}{(1-x_3)^2} = \frac{\varphi'(1)^2 - \varphi(1)\varphi''(1)}{\varphi(1)^2} =$

3. Chứng minh quy nạp theo n . Rõ ràng mệnh đề đúng khi $n = 0$.
 Giả sử mệnh đề đúng đến n . Khi đó

$$\begin{aligned}(x+1)^{2n+3} + x^{n+3} &= (x+1)^2(x+1)^{2n+1} + x \cdot x^{n+2} \\&= (x^2 + 2x + 1)(x+1)^{2n+1} + x \cdot x^{n+2} \\&= (x^2 + x + 1)(x+1)^{2n+1} + x((x+1)^{2n+1} + x^{n+2}).\end{aligned}$$

Số hạng thứ nhất chia hết cho $x^2 + x + 1$, số hạng thứ hai chia hết cho $x^2 + x + 1$ theo giả thiết quy nạp. Vậy mệnh đề được chứng minh.

4. $x^k = x^{qn+r} = (x^{qn} - 1)x^r + x^r = (x^n - 1) \left(\sum_{j=0}^{q-1} x^{jn+r} \right) + x^r$, trong
 đó $\deg(x^r) = r < n = \deg(x^n - 1)$. Do đó dư của phép chia Euclid x^k
 cho $x^n - 1$ là x^r .

5. Theo phép chia Euclide $(x \sin \varphi + \cos \varphi)^n$ cho $x^2 + 1$, tồn tại $q(x) \in \mathbb{C}[x]$ và $a, b \in \mathbb{C}$ sao cho $(x \sin \varphi + \cos \varphi)^n = (x^2 + 1)q(x) + ax + b$.

Thay x bởi i và $-i$, ta có $\begin{cases} ai + b = \cos(n\varphi) + i \sin(n\varphi), \\ -ai + b = \cos(-n\varphi) + i \sin(-n\varphi). \end{cases}$

Từ đó dư cần tìm là $x \sin(n\varphi) + \cos(n\varphi)$.

6. Sử dụng phép chia Euclid:

$$\begin{aligned}f(x) &= (x+1)g(x) + (2x^2 - x - 1), \\g(x) &= (x-1)(2x^2 - x - 1) + (2x + 1), \\2x^2 - x - 1 &= (x-1)(2x + 1).\end{aligned}$$

Do đó $2x + 1$ là ước chung lớn nhất của $f(x)$ và $g(x)$. Ta có

$$\begin{aligned}2x+1 &= g(x) - (x-1)(2x^2 - x - 1) = g(x) - (x-1)(f(x) - (x+1)g(x)) \\&= g(x) + (x^2 - 1)g(x) - (x-1)f(x) \\&= x^2g(x) - (x-1)f(x).\end{aligned}$$

7. Sử dụng phép chia Euclid:

$$\begin{aligned}f(x) &= (x^2 + x + \bar{1})g(x) + \bar{2}x, \\g(x) &= \bar{2}x(\bar{2}x^2 + x) + x + \bar{1}, \\\bar{2}x &= \bar{2}(x + \bar{1}) + \bar{1}.\end{aligned}$$

Do đó $\bar{1}$ là ước chung lớn nhất của $f(x)$ và $g(x)$.

8. Giả sử $AB + BC + CA$ không nguyên tố cùng nhau với ABC . Khi đó tồn tại đa thức bất khả quy $D \in F[x]$ sao cho $D \mid (AB + BC + CA)$ và $D \mid ABC$. Do D bất khả quy nên $D \mid A$ hoặc $D \mid B$ hoặc $D \mid C$. Giả sử $D \mid A$. Vì $D \mid A$ và $D \mid (AB + BC + CA)$ nên $D \mid BC$ và do

D bất khả quy nên $D \mid B$ hoặc $D \mid C$. Giả sử $D \mid B$. Vậy $D \mid A$ và $D \mid B$. Mâu thuẫn với điều kiện $(A, B) = 1$.

9. Thực hiện liên tiếp phép chia Euclid, ta được $(A, B) = 1$.

Với $U = \frac{1}{2}(x^2 - x + 1)$, $V = -\frac{1}{2}(x^3 - x^2 + x + 1)$, ta có $AU + BV = 1$.

10. a) Thay x bằng $x + 1$, ta có

$$(x+1)^4 - 13(x+1)^3 + 45(x+1)^2 - 61(x+1) + 25 = x^4 - 9x^3 + 12x^2 - 6x - 3.$$

Đa thức này bất khả quy trong $\mathbb{Q}[x]$ theo tiêu chuẩn Eisenstein với $p = 3$.

b) Thay x bằng $x + 1$, ta có

$$(x+1)^4 + (x+1)^3 + (x+1)^2 + (x+1) + 1 = x^4 + 5x^3 + 10x^2 + 10x + 5.$$

Đa thức này bất khả quy trong $\mathbb{Q}[x]$ theo tiêu chuẩn Eisenstein với $p = 5$.

11. a) Thay x bằng $x + 2$, ta có

$$(x+2)^3 - 3(x+2) + 1 = x^3 + 6x^2 + 9x + 3.$$

Đa thức này bất khả quy trong $\mathbb{Q}[x]$ theo tiêu chuẩn Eisenstein với $p = 3$.

b) $f(x)$ có bậc 3 trong $\mathbb{Q}[x]$ nên $f(x)$ là bất khả quy trong $\mathbb{Q}[x]$ khi và chỉ khi $f(x)$ vô nghiệm trong \mathbb{Q} .

Giả sử $f(x)$ có nghiệm hữu tỉ là $q \in \mathbb{Q}$. Khi đó $q^3 - 3n^2q + n^3 = 0$ hay $\left(\frac{q}{n}\right)^3 - 3\left(\frac{q}{n}\right) + 1 = 0$. Như vậy $\frac{q}{n}$ là nghiệm của đa thức $x^3 - 3x + 1$. Điều này mâu thuẫn với 1).

12.

$$\begin{aligned} (b-a)^{2n-1} &= ((x-a) - (x-b))^{2n-1} \\ &= \sum_{k=0}^{2n-1} C_{2n-1}^k (-1)^k (x-a)^{2n-1-k} (x-b)^k \\ &= \left(\sum_{k=0}^{n-1} C_{2n-1}^k (-1)^k (x-a)^{n-1-k} (x-b)^k \right) (x-a)^n + \\ &\quad + \left(\sum_{k=n}^{2n-1} C_{2n-1}^k (-1)^k (x-a)^{2n-1-k} (x-b)^{k-n} \right) (x-b)^n. \end{aligned}$$

Từ đó ta có $U(x-a)^n + V(x-b)^n = 1$, trong đó

$$\begin{cases} U &= \frac{1}{(b-a)^{2n-1}} \sum_{k=0}^{n-1} C_{2n-1}^k (-1)^k (x-a)^{n-1-k} (x-b)^k, \\ V &= \frac{1}{(b-a)^{2n-1}} \sum_{l=0}^{n-1} C_{2n-1}^{n+l} (-1)^{n+l} (x-a)^{n-1-l} (x-b)^l. \end{cases}$$

13. Giả sử $f(x)$ là khả quy trên \mathbb{Q} . Khi đó $f(x)$ có thể phân tích được thành tích của hai đa thức bậc hai:

$$x^4 + px^2 + q = (x^2 + ax + m)(x^2 + bx + n).$$

So sánh hệ số ở hai vế, ta suy ra

$$\begin{cases} a+b &= 0, \\ m+n+ab &= p, \\ an+bm &= 0, \\ mn &= q. \end{cases}$$

Nếu $a = 0$ thì $b = 0$ và $\begin{cases} m+n &= p, \\ mn &= q. \end{cases}$ Khi đó m và n là nghiệm của phương trình $x^2 - px + q = 0$. Phương trình này có nghiệm hữu tỉ khi và chỉ khi $\Delta = p^2 - 4q$ là bình phương của một số hữu tỉ.

Nếu $a \neq 0$ thì $m = n$ và $\begin{cases} a &= -b, \\ 2n - a^2 &= p, \\ n^2 &= q. \end{cases}$ Vì a và n là những

số hữu tỉ nên q , $2\sqrt{q} - p$ phải là bình phương của những số hữu tỉ.

Từ các kết quả trên suy ra rằng đa thức $x^4 + px^2 + q$ là bất khả quy trên \mathbb{Q} khi và chỉ khi q , $p^2 - 4q$ và $2\sqrt{q} - p$ không phải là bình phương của những số hữu tỉ.

14. Giả sử $f(x) = (x - a_1)(x - a_2) \dots (x - a_n) - 1$ với a_i là những số nguyên phân biệt, $i = 1, \dots, n$, không phải là bất khả quy trên \mathbb{Q} . Khi đó tồn tại hai đa thức $g(x)$ và $h(x)$ trong $\mathbb{Z}[x]$ sao cho

$$(1) \quad f(x) = g(x)h(x), \text{ với } 0 < \deg(g(x)), \deg(h(x)) < \deg(f(x)).$$

Từ đẳng thức (1) suy ra $f(a_i) = g(a_i)h(a_i) = -1$, với $i = 1, \dots, n$. Vì $g(a_i), h(a_i) \in \mathbb{Z}$ nên $g(a_i) = -h(a_i)$, với $i = 1, \dots, n$.

Đặt $k(x) = g(x) + h(x)$. Nếu $k(x) = 0$ thì ta có $g(x) = -h(x)$, như vậy $f(x) = -(g(x))^2$. Hệ số dẫn đầu của $f(x)$ bằng 1, còn hệ số dẫn đầu của $-(g(x))^2$ luôn âm. Điều này không thể xảy ra. Nếu $k(x) \neq 0$ thì $\deg(k(x)) < n$, nhưng $k(a_i) = g(a_i) + h(a_i) = 0$, $i = 1, \dots, n$. Vậy $k(x)$ có n nghiệm phân biệt, mâu thuẫn với $\deg(k(x)) < n$.

15. Gọi j và j^2 là hai căn bậc ba phức của đơn vị (tức là hai nghiệm phức của $1 + x + x^2$). Thay x lần lượt bởi $1, j, j^2$ vào đẳng thức $P(x^3) + xQ(x^3) = (1 + x + x^2)R(x)$, ta có:

$$\begin{cases} P(1) + Q(1) = 3R(1) \\ P(1) + jQ(1) = 0 \\ P(1) + j^2Q(1) = 0 \end{cases} \Leftrightarrow \begin{cases} P(1) = 0 \\ Q(1) = 0 \\ R(1) = 0 \end{cases}$$

Vậy $x - 1$ chia hết P, Q, R .

16. a) Do $x^3 + x - 2 = (x - 1)(x^2 + x + 2)$ nên α và β là hai nghiệm phức của $x^2 + x + 2$. Từ đó $\alpha + \beta = -1$, $\alpha\beta = 2$.

Giả sử $B(x) = ax^2 + bx + c$, với $a, b, c \in \mathbb{Q}$, $a \neq 0$. Ta có:

$$\begin{aligned} & \begin{cases} B(1) = 1 \\ B(\alpha) = \beta \\ B(\beta) = \alpha \end{cases} \Leftrightarrow \begin{cases} a + b + c = 1 \\ a\alpha^2 + b\alpha + c = \beta \\ a\beta^2 + b\beta + c = \alpha \end{cases} \\ & \Leftrightarrow \begin{cases} a + b + c = 1 \\ a(\alpha + \beta) + b = -1 \\ a((\alpha + \beta)^2 - 2\alpha\beta) + (b - 1)(\alpha + \beta) + 2c = 0 \end{cases} \\ & \Leftrightarrow \begin{cases} a + b + c = 1 \\ -a + b = -1 \\ -3a - b + 1 + 2c = 0 \end{cases} \Leftrightarrow \begin{cases} a = \frac{3}{4} \\ b = -\frac{1}{4} \\ c = \frac{1}{2} \end{cases}. \end{aligned}$$

Do đó $B(x) = \frac{3}{4}x^2 - \frac{1}{4}x + \frac{1}{2}$.

$$\begin{aligned} b) B(B(x)) - x &= \frac{3}{4}\left(\frac{3}{4}x^2 - \frac{1}{4}x + \frac{1}{2}\right)^2 - \frac{1}{4}\left(\frac{3}{4}x^2 - \frac{1}{4}x + \frac{1}{2}\right) + \frac{1}{2} - x \\ &= \frac{9}{64}(3x^4 - 2x^3 + 3x^2 - 8x + 4) = \frac{9}{64}(3x - 2)(x^3 + x - 2). \end{aligned}$$

Do đó $A(x)$ chia hết $B(B(x)) - x$.

17. P có n nghiệm trong \mathbb{C} . Giả sử n nghiệm của P đều là số thực. Áp dụng Định lý Rolle liên tiếp ta nhận được một nghiệm thực của $P^{(n-2)}$, với

$$P^{(n-2)} = \frac{n!}{2}x^2 + (n-1)!x + (n-2)! = \frac{(n-2)!}{2}(n(n-1)x^2 + 2(n-1)x + 2).$$

Điều này vô lý vì tam thức bậc hai ở trên có biệt thức $\Delta = (n - 1)^2 - 2n(n - 1) = 1 - n^2 < 0$.

18. Với $P \in \mathbb{R}[x]$, theo phép chia Euclid P cho $x^2(x - 1)^2$, tồn tại $Q \in \mathbb{R}[x]$ và $a, b, c, d \in \mathbb{R}$ sao cho $P = x^2(x - 1)^2Q + ax^3 + bx^2 + cx + d$. Ta có:

$$\begin{cases} P(0) = 1 \\ P(1) = 0 \\ P'(0) = 0 \\ P'(1) = 1 \end{cases} \Leftrightarrow \begin{cases} d = 1 \\ a + b + c + d = 0 \\ c = 0 \\ 3a + 2b + c = 1 \end{cases} \Leftrightarrow \begin{cases} a = 3 \\ b = -4 \\ c = 0 \\ d = 1 \end{cases}.$$

Vậy các đa thức cần tìm là $P = x^2(x - 1)^2Q + 3x^3 - 4x^2 + 1$, với $Q \in \mathbb{R}[x]$ tùy ý.

19. Ta dùng phương pháp chia Euclid liên tiếp:

$$\begin{aligned} -x^5 + 2x^4 - 4x^3 + 5x^2 - 4x + 3 &= (-x^3 + 2x^2 - 3x + 3)(x^2 + 1) - x \\ -x^3 + 2x^2 - 3x + 3 &= (-x + 2)(x^2 + 1) + (-2x + 1). \end{aligned}$$

Do đó

$$\frac{-x^5 + 2x^4 - 4x^3 + 5x^2 - 4x + 3}{(x^2 + 1)^3} = \frac{-x}{(x^2 + 1)^3} + \frac{-2x + 1}{(x^2 + 1)^2} + \frac{-x + 2}{(x^2 + 1)}.$$

20. $\frac{\bar{2}x^5 + \bar{3}x^3 + \bar{6}x^2 + \bar{3}}{(x^2 + \bar{1})^2} = \bar{2}x + \frac{\bar{6}x^3 + \bar{6}x^2 + \bar{5}x + \bar{3}}{(x^2 + \bar{1})^2}$. Do $x^2 + \bar{1}$ là bất khả quy trên \mathbb{Z}_7 và $\bar{6}x^3 + \bar{6}x^2 + \bar{5}x + \bar{3} = (\bar{6}x + \bar{6})(x^2 + \bar{1}) + (\bar{6}x + \bar{4})$, ta có:

$$\frac{\bar{2}x^5 + \bar{3}x^3 + \bar{6}x^2 + \bar{3}}{(x^2 + \bar{1})^2} = \bar{2}x + \frac{\bar{6}x + \bar{6}}{x^2 + \bar{1}} + \frac{\bar{6}x + \bar{4}}{(x^2 + \bar{1})^2}.$$

$$21. \frac{\bar{2}x^5 + \bar{3}x^3 + x^2 + \bar{1}}{(x^2 + \bar{1})^2} = \bar{2}x + \frac{\bar{4}x^3 + x^2 + \bar{3}x + \bar{1}}{(x^2 + \bar{1})^2}$$

Ta có phân tích $x^2 + \bar{1} = (x - \bar{2})(x - \bar{3})$ trong $\mathbb{Z}_5[x]$. Do đó

$$\frac{\bar{4}x^3 + x^2 + \bar{3}x + \bar{1}}{(x^2 + \bar{1})^2} = \frac{a}{x - \bar{2}} + \frac{b}{(x - \bar{2})^2} + \frac{c}{x - \bar{3}} + \frac{d}{(x - \bar{3})^2}$$

hay $\bar{4}x^3 + x^2 + \bar{3}x + \bar{1} = a(x - \bar{2})(x - \bar{3})^2 + b(x - \bar{3})^2 + c(x - \bar{3})(x - \bar{2})^2 + d(x - \bar{2})^2$. Đặt x lần lượt bằng $\bar{2}$ và $\bar{3}$, ta được $b = \bar{3}$, $d = \bar{2}$.

Đồng nhất hệ số cao nhất và xét số hạng tự do của hai vế ta được
 $a + c = \bar{4}$, $a - c = \bar{3}$. Từ đó $a = \bar{1}$, $c = \bar{3}$. Vậy trên \mathbb{Z}_5 , ta có

$$\frac{\bar{2}x^5 + \bar{3}x^3 + x^2 + \bar{1}}{(x^2 + \bar{1})^2} = \bar{2}x + \frac{\bar{1}}{x - \bar{2}} + \frac{\bar{3}}{(x - \bar{2})^2} + \frac{\bar{3}}{x - \bar{3}} + \frac{\bar{2}}{(x - \bar{3})^2}.$$

22. a) $f(x) = (1 - x^2)^3 - (-2x)^3 = 0 \Leftrightarrow (1 - x^2)^3 = (-2x)^3 \Leftrightarrow 1 - x^2 + 2x = 0$ hoặc $1 - x^2 + 2jx = 0$ hoặc $1 - x^2 + 2j^2x = 0$, trong đó j và j^2 là các căn bậc 3 phức của đơn vị. Do đó phương trình đã cho có 6 nghiệm:
 $x_1 = 1 + \sqrt{2}$, $x_2 = 1 - \sqrt{2}$, $x_3 = \frac{\sqrt{3} - 1}{2} + i\frac{\sqrt{3} - 1}{2}$, $x_4 = \frac{-\sqrt{3} - 1}{2} + i\frac{\sqrt{3} + 1}{2}$,
 $x_5 = \frac{\sqrt{3} - 1}{2} - i\frac{\sqrt{3} - 1}{2}$, $x_6 = \frac{-\sqrt{3} - 1}{2} - i\frac{\sqrt{3} + 1}{2}$.

b)

$$\begin{aligned} f(x) &= (x - x_1)(x - x_2)(x - x_3)(x - x_5)(x - x_4)(x - x_6) \\ &= (x - 1 - \sqrt{2})(x - 1 + \sqrt{2})[x^2 + (\sqrt{3} - 1)x + (2 - \sqrt{3})] \\ &\quad \cdot [x^2 + (\sqrt{3} + 1)x + (2 + \sqrt{3})] \end{aligned}$$

là phân tích thành tích những đa thức bất khả quy hệ số thực.

23. $x^5 + 1$ có các nghiệm phức là

$$u_k = \cos \frac{\pi + 2k\pi}{5} + i \sin \frac{\pi + 2k\pi}{5}, \quad k = 0, 1, 2, 3, 4.$$

$$* k = 2 : u_2 = -1, P(-1) = 0.$$

* $k = 0, 1, 3, 4$: $u_k \neq -1$. Do $u_k^4 - u_k^3 + u_k^2 - u_k + 1 = \frac{u_k^5 + 1}{u_k + 1} = 0$,
ta có $u_k^4 = u_k^3 - u_k^2 + u_k - 1$. Từ đó với mỗi $k = 0, 1, 3, 4$,

$$\begin{aligned} P_n(u_k) &= (u_k^4 - 1)(u_k^3 - u_k^2 + u_k - 1)^n + (u_k + 1)u_k^{4n-1} \\ &= (u_k^4 - 1)(u_k^4)^n + (u_k + 1)u_k^{4n-1} = u_k^{4n-1}((u_k^5 - u_k) + (u_k + 1)) \\ &= 0. \end{aligned}$$

Vậy A chia hết P_n .

24. Ký hiệu Q và R là thương và dư của phép chia Euclid A cho B :

$$A = BQ + R, \deg R \leq 3.$$

Vì $\begin{cases} R(a) = A(a) = (a - b)^{2n} \\ R(b) = A(b) = (b - a)^{2n} \end{cases}$, nên tồn tại $S \in \mathbb{C}[x]$ sao cho

$$R - (b - a)^{2n} = (x - a)(x - b)S, \deg(S) \leq 1.$$

Hơn nữa, lấy đạo hàm: $A' = B'Q + BQ' + R'$, từ đó ta có:

$$\begin{cases} 2n(a - b)^{2n-1} = A'(a) = R'(a) = (a - b)S(a) \\ 2n(b - a)^{2n-1} = A'(b) = R'(b) = (b - a)S(b) \end{cases}$$

Do đó $S(a) = S(b) = 2n(b - a)^{2n-2}$. Vì $\deg S \leq 1$, ta được $S = 2n(b - a)^{2n-2}$. Vậy $R = 2n(b - a)^{2n-2}(x - a)(x - b) + (b - a)^{2n}$.

25. Ký hiệu $A = \sum_{i=0}^{n-1} x^i$ và $B = \left(\sum_{i=0}^n x^i \right)^p - x^n$.

$$\text{Ta có } B = (A + x^n)^p - x^n = \sum_{k=1}^p C_p^k A^k (x^n)^{p-k} + (x^{np} - x^n)$$

$$\text{và } x^{np} - x^n = (x^n - 1) \sum_{k=0}^{p-1} (x^n)^k = A(x - 1) \sum_{k=0}^{p-1} (x^n)^k.$$

Vậy A chia hết B .

26. $x^{2n+1} + (x + 1)^{n+2} = (x^2 + x + 1)P + ax + b$. Với j là một căn bậc 3 phức của đơn vị, thay j vào đẳng thức này, ta có

$$aj + b = j^{2n+1} + (j + 1)^{n+2} = j^{2n+1} + (-j^2)^{n+2},$$

$$aj^2 + b = j^{2(2n+1)} + (j^2 + 1)^{n+2} = j^{2(2n+1)} + (-j)^{n+2}.$$

Do đó

$$ax + b = \begin{cases} 2x & \text{nếu } n = 6k \\ 0 & \text{nếu } n = 6k + 1 \\ -2x - 2 & \text{nếu } n = 6k + 2 \\ 0 & \text{nếu } n = 6k + 3 \\ 2 & \text{nếu } n = 6k + 4 \\ 0 & \text{nếu } n = 6k + 5 \end{cases}$$

27. Ký hiệu $P_n(x) = (x^n + 1)^n - x^n$, ta có $P_n(j) = (j^n + 1)^n - j^n$. Tách trường hợp theo đồng dư modulo 3 của n :

$$P_n(j) = \begin{cases} 2^n - 1 & \text{nếu } n = 3p \\ (-1)^{p+1}j^2 - j & \text{nếu } n = 3p + 1 \\ (-1)^pj^2 - j^2 & \text{nếu } n = 3p + 2 \end{cases}$$

Vậy $n \equiv 2 \pmod{6}$.

28. a) \Rightarrow b): Ký hiệu $D = UCLN(A, B)$, ta có $\deg(D) \leq 1$. Khi đó tồn tại $A_1, B_1 \in \mathbb{F}[x] \setminus \{0\}$ sao cho $A = DA_1$, $B = DB_1$. Ký hiệu $U = B_1$, $V = -A_1$, ta có $AU + BV = 0$, $\deg(U) < \deg(B)$, $\deg(V) < \deg(A)$.

b) \Rightarrow a): Giả sử tồn tại $U, V \in \mathbb{F}[x] \setminus \{0\}$ sao cho $AU + BV = 0$, $\deg(U) < \deg(B)$, $\deg(V) < \deg(A)$. Ký hiệu $D = UCLN(A, B)$. Khi đó tồn tại $A_1, B_1 \in \mathbb{F}[x] \setminus \{0\}$ sao cho

$$A = DA_1, \quad B = DB_1, \quad UCLN(A_1, B_1) = 1.$$

Vì $UA_1 + VB_1 = 0$, nên $A_1 | VB_1$, do đó $A_1 | V$. Vậy tồn tại $P \in \mathbb{F}[x] \setminus \{0\}$ sao cho $V = PA_1$. Từ đó ta có $\deg(A_1) \leq \deg(V) < \deg(A)$ và suy ra $\deg(D) \geq 1$ hay A và B không nguyên tố cùng nhau.

29. Xét ánh xạ $\varphi : (0, +\infty) \rightarrow \mathbb{R}$ cho bởi $\varphi(x) = \frac{P(x)}{x^n} = 1 - \sum_{k=0}^{n-1} \frac{a_k}{x^{n-k}}$. Khi đó φ là một hàm khả vi trên $(0, +\infty)$ và

$$\forall x \in (0, +\infty), \quad \varphi'(x) = \sum_{k=0}^{n-1} \frac{(n-k)a_k}{x^{n+1-k}} > 0.$$

Như vậy, φ tăng thực sự trên $(0, +\infty)$. Ngoài ra, φ liên tục và

$$\lim_{x \rightarrow 0^+} \varphi(x) = -\infty, \quad \lim_{x \rightarrow +\infty} \varphi(x) = 1,$$

do đó tồn tại duy nhất $x_0 \in (0, +\infty)$ sao cho $\varphi(x_0) = 0$.

30. Xét vành thương $\mathbb{F} = \mathbb{Q}[x]/(f(x))$, trong đó $(f(x))$ là iđêan sinh bởi đa thức $f(x)$. Khi đó \mathbb{F} còn là một không gian vectơ trên trường \mathbb{Q} các số hữu tỉ. Do \mathbb{F} là hữu hạn chiều và tập $\{\bar{x}^2, \bar{x}^3, \bar{x}^5, \dots, \bar{x}^p, \dots\}$ là vô hạn (ở đây, với $h(x) \in \mathbb{Q}[x]$, $\overline{h(x)} = h(x) + (f(x))$ là phần tử trong \mathbb{F} và các lũy thừa \bar{x}^p có p là số nguyên tố) nên tập này là phụ thuộc tuyến tính trên \mathbb{Q} . Do đó tồn tại dãy hữu hạn các số hữu tỉ $a_2, a_3, a_5, \dots, a_p$ không đồng thời bằng 0 sao cho

$$a_2\bar{x}^2 + a_3\bar{x}^3 + a_5\bar{x}^5 + \dots + a_p\bar{x}^p = \bar{0}$$

$$\text{hay } a_2x^2 + a_3x^3 + a_5x^5 + \dots + a_px^p \in (f(x))$$

$$\text{hay } a_2x^2 + a_3x^3 + a_5x^5 + \dots + a_px^p = f(x)g(x),$$

với $g(x)$ là một đa thức hệ số hữu tỉ.

31. Tính $P_n(1), P'_n, P'_n(1), P''_n, P''_n(1), \dots$ ta được

* $P_n(1) = 0.$

$$* P'_n = 2nx^{2n-1} - n^2(n+1)x^n + 2n(n^2 - n - 1)x^{n-1} - n^2(n-1)x^{n-2}.$$

* $P'_n(1) = 0.$

$$* P''_n = 2n(2n-1)x^{2n-2} - n^3(n+1)x^{n-1} + 2n(n^2-1)(n-1)x^{n-2} \\ - n^2(n-1)(n-2)x^{n-3}.$$

* $P''_n(1) = 0.$

$$* P_n^{(3)} = 2n(2n-1)(2n-2)x^{2n-3} - n^3(n+1)(n-1)x^{n-2} \\ + 2n(n^2-1)(n-1)(n-2)x^{n-3} - n^2(n-1)(n-2)(n-3)x^{n-4}.$$

* $P_n^{(3)}(1) = 0.$

$$* P_n^{(4)} = 2n(2n-1)(2n-2)(2n-3)x^{2n-4} - n^3(n+1)(n-1)(n-2)x^{n-3} \\ + 2n(n^2-1)(n-1)(n-2)(n-3)x^{n-4} \\ - n^2(n-1)(n-2)(n-3)(n-4)x^{n-5}.$$

* $P^{(4)}(1) \neq 0.$

Vậy 1 là nghiệm của P_n và cấp bội của nó là 4.

32. Giả sử tồn tại $a, b, c \in \mathbb{Z}$ đôi một khác nhau và $P \in \mathbb{Z}[x]$ sao cho $P(a) = b, P(b) = c, P(c) = a$. Vì $P(a) - b = 0$, tồn tại $Q \in \mathbb{Q}[x]$ sao cho $P - b = (x-a)Q$. Phép chia Euclid $P - b$ cho $x - a$ chứng tỏ rằng các hệ số của Q đều thuộc \mathbb{Z} . Thay x bởi b ta có $c - b = (b - a)Q(b)$ và $Q(b) \in \mathbb{Z}$. Do đó $(b - a)|(c - b)$

Hoán vị vòng tròn a, b, c ta được:

$$(b - a)|(c - b), (c - b)|(a - c), (a - c)|(b - a) \Rightarrow |b - a| = |a - c| = |c - b|.$$

Nếu $b - a = c - a$ thì $b = c$: vô lý. Do đó $b - a = a - c$ và tương tự $a - c = c - b$. Vậy $a = b = c$: vô lý.

BÀI TẬP CHƯƠNG IV – MÔĐUN

1. Ký hiệu $M = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y > 0\}$. Chứng minh rằng M là một môđun trên vành các số thực \mathbb{R} với hai phép toán sau:

$$\begin{aligned}\forall (x, y), (u, v) \in M, \forall \alpha \in \mathbb{R}, (x, y) + (u, v) &= (x + u, yv), \\ \alpha(x, y) &= (\alpha x, y^\alpha).\end{aligned}$$

2. Xét môđun trên vành \mathbb{R} các số thực $M_n(\mathbb{R})$ gồm các ma trận vuông cấp n hệ số thực. Ký hiệu $S(n)$ là tập hợp các ma trận đối xứng thực cấp n (tức là $A = (a_{ij}) \in M_n(\mathbb{R})$ mà $a_{ij} = a_{ji}$) và $A(n)$ là tập hợp các ma trận phản đối xứng thực cấp n (tức là $A = (a_{ij}) \in M_n(\mathbb{R})$ mà $a_{ij} = -a_{ji}$). Chứng minh rằng:

- a) $S(n)$ và $A(n)$ là các môđun con của $M_n(\mathbb{R})$.
- b) $M_n(\mathbb{R}) = S(n) \oplus A(n)$.
- c) Tìm cơ sở của $S(3)$ và $A(3)$.

3. Chứng minh rằng một nhópm aben có thể được xem như là một \mathbb{Z} -môđun, với \mathbb{Z} là vành các số nguyên.

4. Một R -môđun M được gọi là nửa đơn nếu mỗi môđun con của M đều là hạng tử trực tiếp của M . Chứng minh rằng mọi môđun con của một môđun nửa đơn là một môđun nửa đơn.

5. Nhópm cộng aben \mathbb{Z} các số nguyên được xem như là một môđun trên chính vành \mathbb{Z} .

- a) Hãy xác định các môđun con của \mathbb{Z} .
- b) Chứng tỏ rằng không tồn tại hai môđun con khác không I và J của \mathbb{Z} sao cho $\mathbb{Z} = I \oplus J$.

6. Cho M là một R -môđun. M gọi là không phân tích được nếu không tồn tại hai môđun con khác không I và J của M sao cho M là tổng trực tiếp của I và J .

Nhópm cộng aben \mathbb{Z}_{15} các số nguyên modulo 15 được xem như là môđun trên vành các số nguyên \mathbb{Z} . Hãy phân tích \mathbb{Z}_{15} thành tổng trực tiếp các môđun con không phân tích được. Sự phân tích trên có duy nhất không?

7. Nhópm cộng aben \mathbb{Q} các số hữu tỉ được xem như là một môđun trên vành \mathbb{Z} các số nguyên. Chứng minh rằng:

- a) Hai phần tử tùy ý của \mathbb{Q} là phụ thuộc tuyến tính trên \mathbb{Z} .

b) \mathbb{Q} không có một cơ sở trên \mathbb{Z} .

8. Chứng minh rằng từ một tập sinh tuỳ ý của \mathbb{Z} -môđun \mathbb{Q} , ta rút ra một phần tử bất kỳ thì tập hợp các phần tử còn lại vẫn là tập sinh của \mathbb{Z} -môđun \mathbb{Q} .

9. Cho R là một vành có đơn vị, R được xem như R -môđun trái và mọi iđéan trái của R được xem như môđun con của R -môđun R . Chứng minh rằng:

a) Nếu I là một iđéan trái của R thì môđun thương R/I là một R -môđun cyclic.

b) Nếu I là một iđéan trái tối đại của R thì môđun thương R/I là một R -môđun đơn.

10. Cho R là một miền nguyên và M là một R -môđun. Với mỗi $x \in M$, ký hiệu $\text{Ann}(x) = \{r \in R \mid rx = 0\}$ (gọi là linh hoá tử của x).

a) Chứng tỏ rằng $T(M) = \{x \in M \mid \text{Ann}(x) \neq \{0\}\}$ là một môđun con của M , gọi là môđun con xoắn của M .

b) Tính $T(M)$ khi $R = \mathbb{Z}$, $M = \mathbb{Z}^2/L$ với $L = ((4, 6))$.

c) M được gọi là không xoắn nếu $T(M) = \{0\}$. Chứng tỏ rằng $M/T(M)$ không xoắn.

d) M được gọi là xoắn nếu $T(M) = M$. Cho N là một R -môđun con của M . Chứng tỏ rằng nếu N và M/N là xoắn thì M là xoắn.

11. Cho R là vành có đơn vị, M là một R -môđun và $a \in R$. Xét ánh xạ $\lambda_a : M \rightarrow M$ xác định bởi $\lambda_a(x) = ax$ với mọi $x \in M$. Hỏi phải chọn a thế nào để λ_a là một tự đồng cấu của R -môđun M ?

12. Cho R là vành có đơn vị 1 và R^2 là môđun tích trên R . Chứng minh rằng mọi đồng cấu R -môđun từ R^2 vào R đều có dạng

$$(x_1, x_2) \mapsto x_1a_1 + x_2a_2,$$

với $a_1, a_2 \in R$ được chọn thích hợp.

13. Cho x, y là các phần tử của vành R có đơn vị $1 \neq 0$ thoả điều kiện $Rx = Ry$. Chứng minh rằng tồn tại một đẳng cấu R -môđun phải

$$f : xR \rightarrow yR \text{ sao cho } f(x) = y.$$

14. Cho hai trường hữu hạn các số nguyên môđulô \mathbb{Z}_{11} và \mathbb{Z}_7 . Ta định nghĩa các phép toán trên $\mathbb{Z}_{11} \times \mathbb{Z}_7^*$, với $\mathbb{Z}_7^* = \mathbb{Z}_7 \setminus \{\bar{0}\}$, như sau:

$$\forall (x, y), (x', y') \in \mathbb{Z}_{11} \times \mathbb{Z}_7^*, \forall n \in \mathbb{Z}, (x, y) + (x', y') = (x + x', y \cdot y'),$$

$$n \cdot (x, y) = (nx, y^n).$$

MATH-EDUCARE

a) Chứng tỏ rằng $\mathbb{Z}_{11} \times \mathbb{Z}_7^*$ là một môđun trên vành các số nguyên \mathbb{Z} .

b) \mathbb{Z}_n là nhóm cộng các số nguyên môđulô n , được xem như là \mathbb{Z} -môđun. Môđun $\mathbb{Z}_{11} \times \mathbb{Z}_7^*$ có đẳng cấu với môđun \mathbb{Z}_{66} không?

c) $\mathbb{Z}_7 \times \mathbb{Z}_{29}^*$ được xem là một \mathbb{Z} -môđun như $\mathbb{Z}_{11} \times \mathbb{Z}_7^*$. Môđun $\mathbb{Z}_7 \times \mathbb{Z}_{29}^*$ có đẳng cấu với môđun \mathbb{Z}_{196} không?

15. Ký hiệu $M(2, \mathbb{Z})$ là \mathbb{Z} -môđun gồm các ma trận vuông cấp 2 hệ số nguyên. Cho $f : M(2, \mathbb{Z}) \rightarrow M(2, \mathbb{Z})$ là ánh xạ xác định bởi

$$f(X) = AX - XA, \quad \text{với } A = \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}.$$

Chứng tỏ rằng f là một đồng cấu \mathbb{Z} -môđun. Hãy xác định $\text{Ker } f$.

16. Ký hiệu $M(2, \mathbb{Z})$ là \mathbb{Z} -môđun gồm các ma trận vuông cấp 2 hệ số nguyên. Cho $f : M(2, \mathbb{Z}) \rightarrow M(2, \mathbb{Z})$ là ánh xạ xác định bởi

$$f(X) = AX + XA, \quad \text{với } A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Chứng tỏ rằng f là một đơn cấu \mathbb{Z} -môđun.

17. Cho R là một vành có đơn vị, I là một iêean của R sao cho $I^n = 0$ và M, N là các R -môđun phải với $f : M \rightarrow N$ là một đồng cấu R -môđun. Chứng minh rằng:

a) f cảm sinh đồng cấu R -môđun $f' : M/MI \rightarrow N/NI$.

b) Nếu f' là một toàn cấu thì f cũng là một toàn cấu.

18. Cho R là một vành có đơn vị, M là một R -môđun sao cho $M = J \oplus W$, trong đó J, W là các R -môđun con của M . Cho $\psi : J \rightarrow W$ là đồng cấu R -môđun, ký hiệu $U_1 = \{x + \psi(x) \mid x \in J\}$. Chứng minh rằng:

a) U_1 là R -môđun con của M và $U_1 \cong J$.

b) $M = U_1 \oplus W$.

19. Xem các nhóm aben như những \mathbb{Z} -môđun. Chứng minh đẳng cấu \mathbb{Z} -môđun sau:

$$(3\mathbb{Z} + 5\mathbb{Z})/5\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z} \cong 3\mathbb{Z}/15\mathbb{Z}.$$

20. Xem các nhóm cyclic hữu hạn như những \mathbb{Z} -môđun. Chứng minh đẳng cấu:

$$\text{Hom}_{\mathbb{Z}}(\mathbb{Z}_m, \mathbb{Z}_n) \cong \mathbb{Z}_{(m,n)},$$

trong đó (m, n) ký hiệu ước chung lớn nhất của m và n .

21. Cho R là một vành giao hoán có đơn vị 1, R được xem như là một môđun trên chính nó và M là một R -môđun. Chứng minh rằng:

$$\text{Hom}_R(R, M) \cong M.$$

22. Cho R là một vành có đơn vị, M là một R -môđun, n là một số nguyên dương và $\varphi_i : M \rightarrow M$ là một đồng cấu R -môđun với mọi $i = 1, \dots, n$ thoả mãn:

$$\varphi_1 + \dots + \varphi_n = id_M, \quad \varphi_i \circ \varphi_j = 0 \quad (\forall i \neq j).$$

Chứng minh rằng:

- a) $\varphi_i^2 = \varphi_i$ với mọi $i = 1, \dots, n$.
- b) M là tổng trực tiếp của các môđun con $M_i = \text{Im} \varphi_i$, $i = 1, \dots, n$.

23. Cho R là một vành có đơn vị, $0 \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow 0$ là dãy khớp các đồng cấu R -môđun (nghĩa là f đơn cấu, g toàn cấu và $\text{Im } f = \text{Ker } g$) và f khả nghịch trái, tức là có đồng cấu R -môđun $\psi : M \rightarrow M'$ sao cho $\psi \circ f = id_{M'}$. Chứng minh rằng:

- a) $M = \text{Im } f \oplus \text{Ker } \psi$.
- b) g khả nghịch phải, tức là có đồng cấu R -môđun $\varphi : M'' \rightarrow M$ sao cho $g \circ \varphi = id_{M''}$.

24. Cho R là một vành có đơn vị, $0 \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow 0$ là dãy khớp các đồng cấu R -môđun (nghĩa là f đơn cấu, g toàn cấu và $\text{Im } f = \text{Ker } g$) và g khả nghịch phải, tức là có đồng cấu R -môđun $\varphi : M'' \rightarrow M$ sao cho $g \circ \varphi = id_{M''}$. Chứng minh rằng:

- a) $M = \text{Ker } g \oplus \text{Im } \varphi$.
- b) f khả nghịch trái, tức là có đồng cấu R -môđun $\psi : M \rightarrow M'$ sao cho $\psi \circ f = id_{M'}$.

25. Cho A, B, C, D là các R -môđun và các đồng cấu R -môđun

$$\begin{aligned} \alpha : A &\rightarrow B, \quad \beta : B \rightarrow D \\ \gamma : A &\rightarrow C, \quad \delta : C \rightarrow D \end{aligned}$$

sao cho $\beta \circ \alpha = \delta \circ \gamma$. Chứng minh rằng nếu γ là toàn cấu và β là đơn cấu, ta có:

a) $\text{Im}(\alpha) = \beta^{-1}(\text{Im}(\delta))$.

b) $\text{Ker}(\delta) = \gamma(\text{Ker}(\alpha))$.

26. a) Cho $\varphi : A \rightarrow A$ là một đồng cấu R -môđun thoả mãn $\varphi \circ \varphi = \varphi$.
Chứng minh rằng $A = \text{Im} \varphi \oplus \text{Ker} \varphi$.

b) Cho $\varphi : A \rightarrow B$ và $\psi : B \rightarrow C$ là hai đồng cấu R -môđun sao cho $\psi \circ \varphi$ là một đẳng cấu. Chứng minh rằng $B = \text{Im} \varphi \oplus \text{Ker} \psi$.

27. Cho R là một vành giao hoán có đơn vị và M, M', N là các R -môđun. Chứng minh các đẳng cấu R -môđun sau:

a) $\text{Hom}_R(N, M \times M') \cong \text{Hom}_R(N, M) \times \text{Hom}_R(N, M')$.

b) $\text{Hom}_R(M \times M', N) \cong \text{Hom}_R(M, N) \times \text{Hom}_R(M', N)$.

28. Cho biểu đồ các đồng cấu R -môđun sau:

$$\begin{array}{ccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow h & & & & \\ & & D & & & & \end{array}$$

trong đó dòng là khớp (tức là $\text{Im} f = \text{Ker} g$, g là toàn cấu) và $h \circ f = 0$.
Chứng minh rằng tồn tại một đồng cấu R -môđun duy nhất $k : C \rightarrow D$ sao cho $k \circ g = h$.

29. Cho biểu đồ các đồng cấu R -môđun sau:

$$\begin{array}{ccccc} & & D & & \\ & & \downarrow h & & \\ 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C \end{array}$$

trong đó dòng là khớp (tức là $\text{Im} f = \text{Ker} g$, f là đơn cấu) và $g \circ h = 0$.
Chứng minh rằng tồn tại một đồng cấu R -môđun duy nhất $k : D \rightarrow A$ sao cho $f \circ k = h$.

30. Cho biểu đồ các đồng cấu R -môđun sau:

$$\begin{array}{ccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ \alpha \downarrow & & \beta \downarrow & & & & \\ A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & & \end{array}$$

trong đó hình vuông là giao hoán (tức là $\beta \circ f = f' \circ \alpha$), dòng trên là khớp và dòng dưới là nửa khớp (tức là $g' \circ f' = 0$). Chứng minh

rằng tồn tại một đồng cấu R -môđun duy nhất $\gamma : C \rightarrow C$ thoả mãn $\gamma \circ g = g' \circ \beta$.

31. Cho biểu đồ các đồng cấu R -môđun sau:

$$\begin{array}{ccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C \\ & & \beta \downarrow & & \gamma \downarrow \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' \end{array}$$

trong đó hình vuông là giao hoán (tức là $\gamma \circ g = g' \circ \beta$), dòng trên là nửa khớp (tức là $g \circ f = 0$) và dòng dưới là khớp. Chứng minh rằng tồn tại một đồng cấu R -môđun duy nhất $\alpha : A \rightarrow A'$ thoả mãn $f' \circ \alpha = \beta \circ f$.

32. Cho biểu đồ các đồng cấu R -môđun sau:

$$\begin{array}{ccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} & D \\ \alpha \downarrow & & \beta \downarrow & & \gamma \downarrow & & \delta \downarrow \\ A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \xrightarrow{h'} & D' \end{array}$$

trong đó hai dòng là khớp (tức là $Im f = Ker g$, $Im g = Ker h$, $Im f' = Ker g'$, $Im g' = Ker h'$), 3 hình vuông là giao hoán (tức là $\beta \circ f = f' \circ \alpha$, $\gamma \circ g = g' \circ \beta$, $\delta \circ h = h' \circ \gamma$), α là một toàn cấu và δ là một đơn cấu. Chứng minh rằng:

- a) $Im \beta = g'^{-1}(Im \gamma)$.
- b) $Ker \gamma = g(Ker \beta)$.

33. Cho biểu đồ các đồng cấu R -môđun sau:

$$\begin{array}{ccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C \longrightarrow 0 \\ & & \alpha \downarrow & & \beta \downarrow & & \gamma \downarrow \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' \longrightarrow 0 \end{array}$$

trong đó hai dòng là khớp (tức là f đơn cấu, $Im f = Ker g$ và g toàn cấu; f' đơn cấu, $Im f' = Ker g'$ và g' toàn cấu), 2 hình vuông là giao hoán (tức là $\beta \circ f = f' \circ \alpha$, $\gamma \circ g = g' \circ \beta$). Chứng minh rằng:

- a) Nếu α và γ là những đơn cấu thì β cũng là đơn cấu.
- b) Nếu α và γ là những toàn cấu thì β cũng là toàn cấu.

34. Cho $\alpha : A \rightarrow B$ và $\varphi : A \rightarrow C$ là những đồng cấu R -môđun thoả mãn φ là một toàn cầu và $\text{Ker}\varphi \subset \text{Ker}\alpha$. Chứng minh rằng tồn tại đồng cấu R -môđun $\lambda : C \rightarrow B$ sao cho:

- a) $\alpha = \lambda \circ \varphi$;
- b) $\text{Im}\lambda = \text{Im}\alpha$;
- c) λ là một đơn cầu khi và chỉ khi $\text{Ker}\varphi = \text{Ker}\alpha$.

35. Cho biểu đồ các đồng cấu R -môđun sau

$$\begin{array}{ccccc} X & \xrightarrow{\varphi} & Y & \xrightarrow{\psi} & Z \\ \alpha \downarrow & & \beta \downarrow & & \gamma \downarrow \\ X' & \xrightarrow{\varphi'} & Y' & \xrightarrow{\psi'} & Z' \end{array}$$

trong đó hai dòng là khớp và hai hình vuông là giao hoán. Chứng minh rằng:

- a) φ và ψ cảm sinh dãy các đồng cấu R -môđun:

$$(1) \quad \text{Ker}\alpha \longrightarrow \text{Ker}\beta \longrightarrow \text{Ker}\gamma.$$

- b) φ' và ψ' cảm sinh dãy các đồng cấu R -môđun:

$$(2) \quad \text{Im}\alpha \longrightarrow \text{Im}\beta \longrightarrow \text{Im}\gamma.$$

- c) Dãy (1) là khớp nếu φ' là đơn cầu.

Dãy (2) là khớp nếu φ là toàn cầu.

TRẢ LỜI VÀ HƯỚNG DẪN GIẢI BÀI TẬP

CHƯƠNG IV – MÔĐUN

1. $\forall (x, y), (u, v), (t, w) \in M, \forall \alpha, \beta \in \mathbb{R}$,

$$\begin{aligned}(x, y) + (u, v) &= (x + u, yv) = (u + x, vy) \\&= (u, v) + (x, y)\end{aligned}$$

$$\begin{aligned}((x, y) + (u, v)) + (t, w) &= (x + u, yv) + (t, w) = (x + u + t, yvw) \\&= (x, y) + (u + t, vw) \\&= (x, y) + ((u, v) + (t, w))\end{aligned}$$

$$(x, y) + (0, 1) = (x + 0, y1) = (x, y)$$

$$(x, y) + (-x, y^{-1}) = (x - x, yy^{-1}) = (0, 1)$$

$$\begin{aligned}\alpha((x, y) + (u, v)) &= \alpha(x + u, yv) = (\alpha(x + u), (yv)^\alpha) \\&= (\alpha x + \alpha u, y^\alpha v^\alpha) \\&= (\alpha x, y^\alpha) + (\alpha u, v^\alpha) = \alpha(x, y) + \alpha(u, v)\end{aligned}$$

$$\begin{aligned}(\alpha + \beta)(x, y) &= ((\alpha + \beta)x, y^{\alpha+\beta}) = (\alpha x + \beta x, y^\alpha y^\beta) \\&= (\alpha x, y^\alpha) + (\beta x, y^\beta) = \alpha(x, y) + \beta(x, y)\end{aligned}$$

$$\alpha(\beta(x, y)) = \alpha(\beta x, y^\beta) = (\alpha\beta x, (y^\beta)^\alpha) = \alpha\beta(x, y)$$

$$1(x, y) = (1.x, y^1) = (x, y)$$

2.

a) Ta có ma trận 0 thuộc $S(n)$ và $A(n)$ nên $S(n) \neq \emptyset$ và $A(n) \neq \emptyset$. $\forall A, B \in S(n)$ (t.ux. $A, B \in A(n)$), $\forall \alpha, \beta \in \mathbb{R}$,

$$(\alpha A + \beta B)^t = (\alpha A)^t + (\beta B)^t = \alpha A^t + \beta B^t = \alpha A + \beta B \text{ hay } \alpha A + \beta B \in S(n)$$

$$(\text{t.ux. } (\alpha A + \beta B)^t = (\alpha A)^t + (\beta B)^t = \alpha A^t + \beta B^t = -\alpha A - \beta B \text{ hay } \alpha A + \beta B \in A(n)).$$

Vậy $S(n)$ và $A(n)$ là các môđun con của $M_n(\mathbb{R})$.

b) $\forall A \in M_n(\mathbb{R})$, đặt $B = \frac{A + A^t}{2}$ và $C = \frac{A - A^t}{2}$. Ta có

$$B^t = \frac{A^t + (A^t)^t}{2} = \frac{A^t + A}{2} = B \text{ hay } B \in S(n)$$

$$C^t = \frac{A^t - (A^t)^t}{2} = \frac{A^t - A}{2} = -C \text{ hay } C \in A(n)$$

$$A = B + C.$$

Do đó $M_n(\mathbb{R}) = S(n) + A(n)$. Mặt khác,

$$A \in S(n) \cap A(n) \Rightarrow \begin{cases} A^t = A \\ A^t = -A \end{cases} \Rightarrow A = -A \Rightarrow A = 0 \Rightarrow S(n) \cap A(n) = \{0\}.$$

Vậy $M_n(\mathbb{R}) = S(n) \oplus A(n)$.

c) Cơ sở của $S(3)$ và $A(3)$ lần lượt là:

$$\left(\left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{array} \right), \left(\begin{array}{ccc} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{array} \right), \left(\begin{array}{ccc} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{array} \right), \right. \\ \left. \left(\begin{array}{ccc} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{array} \right), \left(\begin{array}{ccc} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{array} \right), \left(\begin{array}{ccc} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{array} \right) \right), \\ \left(\left(\begin{array}{ccc} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{array} \right), \left(\begin{array}{ccc} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{array} \right), \left(\begin{array}{ccc} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{array} \right) \right).$$

3. Cho A là một nhópmaben. Không mất tính chất tổng quát, có thể xem A là một nhómcộngaben. Xét phép nhân vô hướng:

$$\mathbb{Z} \times A \longrightarrow A : (n, x) \mapsto nx = \begin{cases} \underbrace{x + \cdots + x}_{n \text{ lầ}} & \text{nếu } n > 0, \\ 0 & \text{nếu } n = 0, \\ \underbrace{(-x) + \cdots + (-x)}_{-n \text{ lầ}} & \text{nếu } n < 0. \end{cases}$$

Khi đó $\forall x, y \in A, \forall m, n \in \mathbb{Z}$,

$$m(x+y) = mx+my, (m+n)x = mx+nx, m(nx) = (mn)x, 1x = x.$$

Vậy A là một \mathbb{Z} -môđun.

4. Cho M là một R -môđun nửa đơn và N là một môđun con của M . Cho P là một môđun con tùy ý của N . Khi đó P là một môđun con của M và do M là nửa đơn nên tồn tại môđun con Q của M sao cho $M = P \oplus Q$.

Đặt $Q' = Q \cap N$. Khi đó $\forall x \in N, x = y+z$, trong đó $y \in P, z \in Q$ và ta có $z = x - y \in Q \cap N = Q'$. Do đó $N = P \oplus Q'$. Ngoài ra, $P \cap Q' = P \cap Q \cap N = \{0\}$. Từ đó suy ra $N = P \oplus Q'$. Vậy N là một môđun nửa đơn.

5. a) Cho I là một môđun con của \mathbb{Z} . Nếu $I \neq \{0\}$ thì I chứa ít nhất một số nguyên dương. Gọi n là số nguyên dương nhỏ nhất sao cho $n \in I$. Khi đó $\forall m \in I$, $m = nq + r$, với $0 \leq r < n$. Do $r = m - nq \in I$ và tính nhỏ nhất của n , ta có $r = 0$ hay $m = nq \in n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$.

Với $n \in \mathbb{N}$, $n\mathbb{Z}$ là một môđun con của \mathbb{Z} . Thật vậy, rõ ràng $n\mathbb{Z} \neq \emptyset$. $\forall x, y \in n\mathbb{Z}$, $\forall a, b \in \mathbb{Z}$, $\exists k, l \in \mathbb{Z}$, $x = nk, y = nl$, ta có $ax + by = ank + bnl = n(ak + bl) \in n\mathbb{Z}$.

b) Giả sử $\mathbb{Z} = I \oplus J$ với I và J là hai môđun con khác không của \mathbb{Z} . Khi đó tồn tại hai số nguyên dương n và m sao cho $I = n\mathbb{Z}$ và $J = m\mathbb{Z}$. Ta có $nm \neq 0$ và $nm \in n\mathbb{Z} \cap m\mathbb{Z} = I \cap J = \{0\}$. Điều này cho biết \mathbb{Z} không là tổng trực tiếp của hai môđun con khác không I và J .

6. Các môđun con của \mathbb{Z} -môđun \mathbb{Z}_{15} là

$$\{\bar{0}\}, 3\mathbb{Z}_{15} = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \bar{12}\}, 5\mathbb{Z}_{15} = \{\bar{0}, \bar{5}, \bar{10}\},$$

Ở đây, $3\mathbb{Z}_{15}$, $5\mathbb{Z}_{15}$ không có môđun con khác không nào nên chúng là các môđun con không phân tích được. Ngoài ra, ta có

$$\bar{1} = \bar{6} + \bar{10}.$$

Do đó $\mathbb{Z}_{15} = 3\mathbb{Z}_{15} \oplus 5\mathbb{Z}_{15}$ và đây là sự phân tích duy nhất thành tổng trực tiếp các môđun con không phân tích được.

7. a) Nếu lấy hai phần tử, trong đó có phần tử 0 thì hiển nhiên chúng phụ thuộc tuyến tính.

Nếu lấy hai phần tử khác 0: $x = \frac{a}{b}$, $y = \frac{c}{d}$, ($a, b, c, d \in \mathbb{Z} \setminus \{0\}$). Ta có

$$bc\frac{a}{b} = da\frac{c}{d} \Leftrightarrow \alpha x + \beta y = 0, \text{ với } \alpha = bc, \beta = -da \in \mathbb{Z} \setminus \{0\}.$$

Vậy x, y phụ thuộc tuyến tính.

b) Theo trên, muốn có một \mathbb{Z} -cơ sở cho \mathbb{Q} thì cơ sở đó chỉ có thể có 1 phần tử. Giả sử $\mathbb{Q} = \left\langle \frac{a}{b} \right\rangle$ ($a, b \in \mathbb{Z}$). Nhưng điều này không thể được vì nếu $n = \frac{a}{b} \in \mathbb{Z}$ thì $\left\langle \frac{a}{b} \right\rangle = \left\langle n \right\rangle = n\mathbb{Z} \neq \mathbb{Q}$, còn nếu $\frac{a}{b} \notin \mathbb{Z}$ thì $\left\langle \frac{a}{b} \right\rangle = \left\{ \frac{na}{b} \mid n \in \mathbb{Z} \right\} \neq \mathbb{Q}$.

8. Cho X là một tập sinh của \mathbb{Z} -môđun \mathbb{Q} . Lấy $x_0 \in X$ tùy ý và rút nó ra khỏi X . Khi đó $\frac{x_0}{2}$ có thể biểu diễn thành một tổng hữu hạn là:

$$\frac{x_0}{2} = z_0 x_0 + \sum_{x_i \neq x_0} z_i x_i, \quad x_i \in X, z_i \in \mathbb{Z}.$$

Từ đó $x_0 = 2z_0 x_0 + \sum_{x_i \neq x_0} 2z_i x_i$ và $nx_0 = \sum_{x_i \neq x_0} 2z_i x_i$, trong đó $n = 1 - 2z_0 \in \mathbb{Z}$, $n \neq 0$. Tiếp tục, $\frac{x_0}{n}$ có biểu diễn thành tổng hữu hạn:

$$\frac{x_0}{n} = z'_0 x_0 + \sum_{x_i \neq x_0} z'_i x_i, \quad x_i \in X, z'_i \in \mathbb{Z}.$$

Khi đó

$$\begin{aligned} x_0 &= nz'_0 x_0 + \sum_{x_i \neq x_0} nz'_i x_i = \sum_{x_i \neq x_0} 2z_i z'_0 x_i + \sum_{x_i \neq x_0} nz'_i x_i \\ &= \sum_{x_i \neq x_0} z''_i x_i, \quad x_i \in X, \\ z''_i &= 2z_i z'_0 + nz'_i \in \mathbb{Z}. \end{aligned}$$

Điều này cho biết x_0 được biểu diễn qua tập $X \setminus \{x_0\}$. Do X là hệ sinh của \mathbb{Q} nên $X \setminus \{x_0\}$ cũng là hệ sinh của \mathbb{Q} .

9. a) Mỗi phần tử của môđun thương R/I có dạng $x + I$, với $x \in R$ và $x + I = x \cdot 1 + I = x(1 + I)$. Do đó R/I là một R -môđun cyclic sinh bởi $1 + I$.

b) Mỗi môđun con của môđun thương R/I có dạng J/I , với J là idéan trái của R và chứa I . Do I là cực đại, ta có $J = R$ hoặc $J = I$, tức là J/I hoặc là môđun R/I hoặc là môđun không. Vậy R/I là một R -môđun đơn.

10. a) Rõ ràng $0 \in T(M)$ hay $T(M) \neq \emptyset$.

$\forall x, y \in T(M)$, $\forall \alpha, \beta \in R$, $\exists r, s \in R$, $r \neq 0$, $s \neq 0$ sao cho $rx = 0$ và $sy = 0$. Khi đó do R là một miền nguyên nên $rs \neq 0$ và

$$rs(\alpha x + \beta y) = s\alpha(rx) + r\beta(sy) = 0 + 0 = 0 \text{ hay } \alpha x + \beta y \in T(M).$$

Vậy $T(M)$ là một môđun con của M .

b)

$$\begin{aligned}
 T(M) &= \{(k, l) + L \in \mathbb{Z}^2/L \mid \exists n \in \mathbb{Z} \setminus \{0\}, n(k, l) \in ((4, 6))\} \\
 &= \{(k, l) + L \in \mathbb{Z}^2/L \mid \exists n \in \mathbb{Z} \setminus \{0\}, \exists m \in \mathbb{Z}, n(k, l) = m(4, 6)\} \\
 &= \{(k, l) + L \in \mathbb{Z}^2/L \mid \exists n \in \mathbb{Z} \setminus \{0\}, \frac{nk}{2} = \frac{nl}{3} \in \mathbb{Z}\} \\
 &= \{(k, l) + L \in \mathbb{Z}^2/L \mid 3k = 2l\}
 \end{aligned}$$

c)

$$\begin{aligned}
 x + T(M) \in T(M/T(M)) &\Rightarrow \exists r \in R \setminus \{0\}, r(x + T(M)) = T(M) \\
 &\Rightarrow rx \in T(M) \Rightarrow \exists s \in R \setminus \{0\}, s(rx) = 0 \\
 &\Rightarrow \exists rs \in R \setminus \{0\}, (rs)x = 0 \Rightarrow x \in T(M) \\
 &\Rightarrow x + T(M) = T(M) \\
 &\Rightarrow T(M/T(M)) = \{T(M)\}
 \end{aligned}$$

Vậy $M/T(M)$ không xoắn.

d)

$$\begin{aligned}
 N \text{ và } M/N \text{ xoắn} &\Rightarrow \forall x \in M, \exists r \in R \setminus \{0\}, r(x + N) = N \\
 &\Rightarrow \forall x \in M, \exists r \in R \setminus \{0\}, rx \in N \\
 &\Rightarrow \forall x \in M, \exists r, s \in R \setminus \{0\}, s(rx) = 0 \\
 &\Rightarrow \forall x \in M, \exists rs \in R \setminus \{0\}, (rs)x = 0 \\
 &\Rightarrow M \text{ xoắn}
 \end{aligned}$$

11. $\forall x, y \in M, \lambda_a(x+y) = a(x+y) = ax+ay = \lambda_a(x)+\lambda_a(y)$. Do đó λ_a là một đồng cấu R -môđun khi và chỉ khi $\forall r \in R, \forall x \in M, \lambda_a(rx) = r\lambda_a(x)$ hay $a(rx) = r(ax)$ hay $(ar - ra)x = 0$. Như vậy

$\lambda_a \in Hom_R(M, M) \Leftrightarrow a \in \{\alpha \in R \mid (\alpha r - r\alpha)x = 0, \forall r \in R, \forall x \in M\}$.

12. Cho $f : R^2 \rightarrow R$ xác định bởi $f(x_1, x_2) = x_1a_1 + x_2a_2$, với $a_1, a_2 \in R$ nào đó. Khi đó $\forall (x_1, x_2), (y_1, y_2) \in R^2, \forall r, s \in R$,

$$\begin{aligned}
 f(r(x_1, x_2) + s(y_1, y_2)) &= f(rx_1 + sy_1, rx_2 + sy_2) \\
 &= (rx_1 + sy_1)a_1 + (rx_2 + sy_2)a_2 \\
 &= r(x_1a_1 + x_2a_2) + s(y_1a_1 + y_2a_2) \\
 &= rf(x_1, x_2) + sf(y_1, y_2).
 \end{aligned}$$

Do đó f là một đồng cấu R -môđun.

Đảo lại, cho $f : R^2 \rightarrow R$ là một đồng cấu R -môđun. Khi đó $\forall (x_1, x_2) \in R^2$, đặt $a_1 = f(1, 0), a_2 = f(0, 1) \in R$, ta có:

$$\begin{aligned} f(x_1, x_2) &= f((x_1, 0) + (0, x_2)) \\ &= f(x_1(1, 0) + x_2(0, 1)) = x_1 f(1, 0) + x_2 f(0, 1) \\ &= x_1 a_1 + x_2 a_2. \end{aligned}$$

13. Gọi $f : xR \rightarrow yR$ xác định bởi $f(xr) = yr$ với $r \in R$.

Nếu $xr = xr'$ với $r, r' \in R$ thì $x(r - r') = 0$, do $y \in Ry = Rx$ nên $y = r''x$ với $r'' \in R$, vì vậy $y(r - r') = r''x(r - r') = r''0 = 0$ hay $yr = yr'$. Do đó f là một ánh xạ.

$\forall r, r', s, s' \in R$, $f((xr)s + (xr')s') = f(x(rs + r's')) = y(rs + r's') = (yr)s + (yr')s' = f(xr)s + f(xr')s'$. Do đó f là một đồng cấu R -môđun phải.

Rõ ràng f là một toàn ánh.

Cho $xr \in \text{Ker } f$ hay $yr = 0$. Do $x \in Rx = Ry$ nên $x = r'y$ với $r' \in R$ nên $xr = r'yr = r'0 = 0$. Vậy $\text{Ker } f = \{0\}$ hay f là một đơn cấu.

Vậy f là một đồng cấu R -môđun phải.

14. a) Phép cộng trên $\mathbb{Z}_{11} \times \mathbb{Z}_7^*$ có tính giao hoán, kết hợp, có phần tử không là $(\bar{0}, \bar{1})$ và mỗi phần tử $(x, y) \in \mathbb{Z}_{11} \times \mathbb{Z}_7^*$ có phần tử đối là $(-x, y^{-1})$. Ngoài ra, $\forall (x, y), (x', y') \in \mathbb{Z}_{11} \times \mathbb{Z}_7^*$, $\forall n, m \in \mathbb{Z}$,

$$n((x, y) + (x', y')) = n(x + x', yy') = (n(x + x'), (yy')^n) = (nx + nx', y^n y'^n) = (nx, y^n) + (nx', y'^n) = n(x, y) + n(x', y'),$$

$$(n+m)(x, y) = ((n+m)x, y^{n+m}) = (nx + mx, y^n y^m) = (nx, y^n) + (mx, y^m) = n(x, y) + m(x, y),$$

$$n(m(x, y)) = n(mx, y^m) = (nmx, y^{mn}) = nm(x, y),$$

$$1(x, y) = (1x, y^1) = (x, y).$$

Vậy $\mathbb{Z}_{11} \times \mathbb{Z}_7^*$ là một \mathbb{Z} -môđun.

b) \mathbb{Z}_{11} là nhóm cộng cyclic cấp 11, sinh bởi $\bar{0}$ và \mathbb{Z}_7^* là nhóm nhân cyclic cấp 6 sinh bởi $\bar{3}$. Vì $(11, 6) = 1$ nên $\mathbb{Z}_{11} \times \mathbb{Z}_7^*$ là nhóm cyclic cấp $11 \cdot 6 = 66$. Vì vậy, $\mathbb{Z}_{11} \times \mathbb{Z}_7^*$ đồng cấu \mathbb{Z} -môđun với \mathbb{Z}_{66} .

c) $\forall (x, y) \in \mathbb{Z}_7 \times \mathbb{Z}_{29}^*$, $28(x, y) = (28x, y^{28}) = (\bar{0}, \bar{1})$, nên mọi phần tử của $\mathbb{Z}_7 \times \mathbb{Z}_{29}^*$ đều có cấp là ước của 28. Do đó không có phần tử nào của $\mathbb{Z}_7 \times \mathbb{Z}_{29}^*$ có cấp 196, trong khi \mathbb{Z}_{196} là nhóm cyclic cấp 196 nên nó có phần tử cấp 196. Vậy $\mathbb{Z}_7 \times \mathbb{Z}_{29}^*$ không đồng cấu với \mathbb{Z}_{196} .

15. $\forall X, Y \in M(2, \mathbb{Z})$, $\forall a, b \in \mathbb{Z}$,

$$\begin{aligned} f(aX + bY) &= A(aX + bY) - (aX + bY)A \\ &= A(aX) + A(bY) - (aX)A - (bY)A = a(AX) + b(AY) - a(XA) - b(YA) \\ &= a(AX - XA) + b(AY - YA) = af(X) + bf(Y). \end{aligned}$$

Do đó f là một đồng cấu \mathbb{Z} -môđun.

$$\begin{aligned} \text{Ker } f &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2, \mathbb{Z}) \mid f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\} \\ \text{Ker } f &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2, \mathbb{Z}) \mid \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} - \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\} \\ &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2, \mathbb{Z}) \mid \begin{pmatrix} c - 2b & d - a - 3b \\ 2a + 3c - 2d & 2b - c \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\} \\ &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2, \mathbb{Z}) \mid c = 2b, d = a + 3b \right\} \\ &= \left\{ \begin{pmatrix} a & b \\ 2b & a + 3b \end{pmatrix} \mid a, b \in \mathbb{Z} \right\} \\ &= \langle \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} \rangle. \end{aligned}$$

16. $\forall X, Y \in M(2, \mathbb{Z})$, $\forall a, b \in \mathbb{Z}$,

$$\begin{aligned} f(aX + bY) &= A(aX + bY) + (aX + bY)A \\ &= A(aX) + A(bY) + (aX)A + (bY)A = a(AX) + b(AY) + a(XA) + b(YA) \\ &= a(AX + XA) + b(AY + YA) = af(X) + bf(Y). \end{aligned}$$

Do đó f là một đồng cấu \mathbb{Z} -môđun.

$$\begin{aligned} \text{Ker } f &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\} \\ &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \begin{pmatrix} 2a + b & 2b \\ a + 2c + d & b + 2d \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\} \\ &= \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}. \end{aligned}$$

Vậy f là một đơn cấu \mathbb{Z} -môđun.

17. a) Với $x \in MI$, ta có $x = \sum_{i=1}^n m_i a_i$, trong đó $m_i \in M$, $a_i \in I$.

Khi đó $f(x) = \sum_{i=1}^n f(m_i)a_i$, nên $f(x) \in NI$. Từ đó với $x_1, x_2 \in M$, $x_1 + MI = x_2 + MI$, ta có $x_1 - x_2 \in MI$, do đó $f(x_1 - x_2) \in NI$ hay $f(x_1) + NI = f(x_2) + NI$. Vì vậy, ta có ánh xạ $f' : M/MI \rightarrow N/NI$ xác định bởi $f(x + MI) = f(x) + NI$. Kiểm tra đồng cấu R -môđun là dễ dàng.

b) Từ lập luận trên, $f(MI^2) \subset f(NI^2)$ và cảm sinh đồng cấu R -môđun $f'' : M/MI^2 \rightarrow N/NI^2$. Ta chứng minh rằng nếu f' là một toàn cầu thì f'' cũng vậy.

Cho $y \in N$, vì f' là một toàn cầu, tồn tại $x \in M$ sao cho $y + NI = f(x) + NI$. Vậy tồn tại $a_1, \dots, a_n \in I$ và $y_1, \dots, y_n \in N$ sao cho $y = f(x) + \sum_{i=1}^n y_i a_i$. Làm tương tự với mỗi y_i , tồn tại $x_1, \dots, x_n \in M$ mà $y_i = f(x_i) + z_i$, $z_i \in NI$. Từ đó suy ra $y = f(x + \sum_{i=1}^n x_i a_i) + z$, với $z = \sum_{i=1}^n z_i a_i \in NI^2$. Do đó f'' là một toàn cầu.

Quy nạp ta có $f = f^{(n)} : M = M/MI^n \rightarrow N/NI^n = N$ là một toàn cầu.

18. a) $0 = 0 + \psi(0) \in U_1$ nên $U_1 \neq \emptyset$. $\forall a, b \in U_1$, $\forall \alpha, \beta \in R$, $a = x + \psi(x)$, $b = y + \psi(y)$ với $x, y \in U$, ta có:

$$\alpha a + \beta b = \alpha(x + \psi(x)) + \beta(y + \psi(y)) = (\alpha x + \beta y) + \psi(\alpha x + \beta y).$$

Vì $x, y \in U$ nên $\alpha x + \beta y \in U$, do đó $\alpha a + \beta b \in U_1$. Vậy U_1 là một môđun con của M .

Xét ánh xạ $\varphi : U \rightarrow U_1$ cho bởi $\varphi(x) = x + \psi(x)$. Khi đó $\forall x, y \in U$, $\forall \alpha, \beta \in R$, ta có:

$$\begin{aligned}\varphi(\alpha x + \beta y) &= \alpha x + \beta y + \psi(\alpha x + \beta y) = \alpha(x + \psi(x)) + \beta(y + \psi(y)) \\ &= \alpha\varphi(x) + \beta\varphi(y).\end{aligned}$$

Vậy φ là một đồng cấu R -môđun. Rõ ràng φ là một toàn cầu. Ngoài ra,

$$x \in \text{Ker } \varphi \Rightarrow \varphi(x) = 0 \Rightarrow x = -\psi(x) \Rightarrow x \in U \cap W = \{0\} \Rightarrow x = 0.$$

Do đó $\text{Ker } \varphi = \{0\}$ hay φ là một đơn cầu. Vậy φ là một đồng cấu.

b) $\forall z \in M, z = x+y$ với $x \in U, y \in W, z = (x+\psi(x))+(y-\psi(x)).$
 Vì $x+\psi(x) \in U_1, y-\psi(x) \in W$ nên $z \in U_1 + W.$ Do đó $M = U_1 + W.$
 $z \in U_1 \cap W \Rightarrow z = x + \psi(x) \in W, x \in U \Rightarrow x = z - \psi(x) \in U \cap W$
 $\Rightarrow x = 0 \Rightarrow z = 0.$
 Do đó $U_1 \cap W = \{0\}.$ Vậy $M = U_1 \oplus W.$

19. Do $(3, 5) = 1,$ tồn tại $m, n \in \mathbb{Z}$ sao cho $3m + 5n = 1.$ Khi đó
 $\forall x \in \mathbb{Z}, x = 3mx + 5nx \in 3\mathbb{Z} + 5\mathbb{Z},$ nên $\mathbb{Z} = 3\mathbb{Z} + 5\mathbb{Z}.$ Do đó

$$(3\mathbb{Z} + 5\mathbb{Z})/5\mathbb{Z} = \mathbb{Z}/5\mathbb{Z}.$$

Mặt khác, từ định lý đẳng cấu cơ bản, ta có $(3\mathbb{Z} + 5\mathbb{Z})/5\mathbb{Z} \cong 3\mathbb{Z}/3\mathbb{Z} \cap 5\mathbb{Z},$
 mà cũng do $(3, 5) = 1$ ta có $3\mathbb{Z} \cap 5\mathbb{Z} = 15\mathbb{Z}.$ Vậy

$$(3\mathbb{Z} + 5\mathbb{Z})/5\mathbb{Z} \cong 3\mathbb{Z}/15\mathbb{Z}.$$

20. Mỗi đồng cấu $f : \mathbb{Z}_m \rightarrow \mathbb{Z}_n$ xác định giá trị $a = f(\bar{1}) \in \mathbb{Z}_n$ và do $ma = mf(\bar{1}) = f(m\bar{1}) = f(\bar{m}) = f(\bar{0}) = \bar{0}$ nên ta có cấp của a trong \mathbb{Z}_n là một ước của m (do đó là một ước chung của m và n). Đảo lại, phần tử $a \in \mathbb{Z}_n$ có cấp là một ước của m thì phép tương ứng $f : \mathbb{Z}_m \rightarrow \mathbb{Z}_n : \bar{k} \mapsto ka$ là một ánh xạ và khi đó f là một đồng cấu \mathbb{Z} -môđun.

Đặt $d = (m, n), d' = \frac{n}{d}.$ Khi đó

$$\text{Hom}_{\mathbb{Z}}(\mathbb{Z}_m, \mathbb{Z}_n) = \{f_i \mid 0 \leq i \leq d-1\}.$$

Ở đây, $f_i : \mathbb{Z}_m \rightarrow \mathbb{Z}_n$ cho bởi $f_i(\bar{1}) = \bar{id'}$ và $f_i = if_1.$ Vậy,

$$\text{Hom}_{\mathbb{Z}}(\mathbb{Z}_m, \mathbb{Z}_n) \cong d'\mathbb{Z}_n \cong \mathbb{Z}_d.$$

21. Xét ánh xạ $\varphi : \text{Hom}_R(R, M) \rightarrow M$ cho bởi $\varphi(f) = f(1).$ Khi đó:

$$\begin{aligned} \forall f, g \in \text{Hom}_R(R, M), \forall a, b \in R, \varphi(af + bg) &= (af + bg)(1) \\ &= af(1) + bg(1) \\ &= a\varphi(f) + b\varphi(g). \end{aligned}$$

Do đó φ là một đồng cấu R -môđun.

$\forall f \in \text{Hom}_R(R, M), \varphi(f) = f(1) = 0$ kéo theo $f(a) = f(a \cdot 1) = af(1) = a0 = 0, \forall a \in R.$ Do đó $\text{Ker}\varphi = \{0\}$ hay φ là một đơn cấu.

MATH-EDUCARE

$\forall x \in M$, xét ánh xạ $f_x : R \longrightarrow M$ cho bởi $f_x(a) = ax$. Khi đó $\forall a, b, \alpha, \beta \in R$, $f_x(\alpha a + \beta b) = (\alpha a + \beta b)x = \alpha(ax) + \beta(bx) = \alpha f_x(a) + \beta f_x(b)$ hay $f_x \in \text{Hom}_R(R, M)$ và $\varphi(f_x) = f_x(1) = 1 \cdot x = x$. Do đó φ là một toàn cầu.

Vậy φ là một đẳng cấu R -môđun.

22. a) Với mọi $i = 1, \dots, n$, ta có

$$\varphi_i = \varphi_i \circ id_M = \varphi_i \circ (\varphi_1 + \dots + \varphi_n) = \varphi_i \circ \varphi_i = \varphi_i^2.$$

b) $\forall x \in M$, $x = id_M(x) = (\varphi_1 + \dots + \varphi_n)(x) = \varphi_1(x) + \dots + \varphi_n(x)$, với $\varphi_i(x) \in M_i$. Do đó $M = M_1 + \dots + M_n$.

Với mỗi $i = 1, \dots, n$, $\forall x \in M_i \cap \sum_{j \neq i} M_j$, ta có $x = x_i = \sum_{j \neq i} x_j$, $x_k \in M_k = \varphi_k(M)$ ($1 \leq k \leq n$), nên $\exists y_k \in M$ sao cho $x_k = \varphi_k(y_k)$ và

$$\varphi_k(x_k) = \varphi_k^2(y_k) = \varphi_k(y_k) = x_k,$$

$$x = x_i = \varphi_i(x_i) = \varphi_i\left(\sum_{j \neq i} \varphi_j(x_j)\right) = \sum_{j \neq i} \varphi_i \circ \varphi_j(x_j) = 0.$$

Do đó $M_i \cap \sum_{j \neq i} M_j = \{0\}$. Vậy $M = M_1 \oplus \dots \oplus M_n$.

23. a) $\forall x \in M$, đặt $y = f(\psi(x))$, $z = x - y$, ta có $\psi(z) = \psi(x - f(\psi(x))) = \psi(x) - \psi(f(\psi(x))) = \psi(x) - \psi(x) = 0$ hay $z \in \text{Ker}\psi$. Do đó $\forall x \in M$, $\exists y \in \text{Im}f$, $\exists z \in \text{Ker}\psi$, $x = y + z$ hay $M = \text{Im}f + \text{Ker}\psi$.

$$x \in \text{Im}f \cap \text{Ker}\psi \Rightarrow x = f(u), u \in M' \text{ và } \psi(x) = 0$$

$$\Rightarrow u = \psi(f(u)) = \psi(x) = 0 \Rightarrow x = 0.$$

Do đó $\text{Im}f \cap \text{Ker}\psi = \{0\}$. Vậy $M = \text{Im}f \oplus \text{Ker}\psi$.

b) Xét đồng cấu $g' = g|_{\text{Ker}\psi} : \text{Ker}\psi \longrightarrow M''$. Ta có:

$$g'(\text{Ker}\psi) = g(\text{Im}f \oplus \text{Ker}\psi) = g(M) = M''$$

$$\text{Ker}g' = \text{Ker}g \cap \text{Ker}\psi = \text{Im}f \cap \text{Ker}\psi = \{0\}.$$

Do đó g' là một đồng cấu R -môđun. Đặt $\varphi = (g')^{-1}$, ta có φ là một đồng cấu R -môđun và kiểm tra dễ dàng $g \circ \varphi = id_{M''}$.

24. a) $\forall x \in M$, đặt $y = \varphi(g(x))$, $z = x - y$, ta có $g(z) = g(x - \varphi(g(x))) = g(x) - g(\varphi(g(x))) = g(x) - g(x) = 0$ hay $z \in \text{Ker}g$. Do đó $\forall x \in M$, $\exists z \in \text{Ker}g$, $\exists y \in \text{Im}\varphi$, $x = z + y$ hay $M = \text{Ker}g + \text{Im}\varphi$.

$$x \in \text{Ker}g \cap \text{Im}\varphi \Rightarrow x = \varphi(u), u \in M'' \text{ và } g(x) = 0$$

$$\Rightarrow u = g(\varphi(u)) = g(x) = 0 \Rightarrow x = 0.$$

Do đó $\text{Kerg} \cap \text{Im}\varphi = \{0\}$. Vậy $M = \text{Kerg} \oplus \text{Im}\varphi$.

b) Do f là đơn cấu và $\text{Im}f = \text{Kerg}$, nên $f : M' \rightarrow \text{Kerg}$ là một đẳng cấu. Xét ánh xạ $\psi : M \rightarrow M'$ xác định bởi $\psi|_{\text{Kerg}} = f^{-1}$, $\psi|_{\text{Im}\varphi} = 0$. Khi đó ψ là một đồng cấu R -môđun và kiểm tra dễ dàng $\psi \circ f = id_{M'}$.

25. a) $b \in \text{Im}\alpha \Rightarrow \exists a \in A, b = \alpha(a) \Rightarrow \beta(b) = \beta(\alpha(a)) = \delta(\gamma(a)) \in \text{Im}\delta \Rightarrow b \in \beta^{-1}(\text{Im}\delta)$. Do đó $\text{Im}\alpha \subset \beta^{-1}(\text{Im}\delta)$.

$b \in \beta^{-1}(\text{Im}\delta) \Rightarrow \beta(b) \in \text{Im}\delta \Rightarrow \exists c \in C, \beta(b) = \delta(c) \Rightarrow \exists a \in A, \gamma(a) = c$ và $\beta(b) = \delta(\gamma(a)) = \beta(\alpha(a)) \Rightarrow b = \alpha(a) \in \text{Im}\alpha$. Do đó $\beta^{-1}(\text{Im}\delta) \subset \text{Im}\alpha$.

Vậy $\text{Im}\alpha = \beta^{-1}(\text{Im}\delta)$.

b) $c \in \text{Ker}\delta \Rightarrow \exists a \in A, \gamma(a) = c$ và $\delta(c) = 0 \Rightarrow \beta(\alpha(a)) = \delta(\gamma(a)) = \delta(c) = 0 \Rightarrow \alpha(a) = 0 \Rightarrow a \in \text{Ker}\alpha$ và $c = \gamma(a) \in \gamma(\text{Ker}\alpha)$. Do đó $\text{Ker}\delta \subset \gamma(\text{Ker}\alpha)$.

$c \in \gamma(\text{Ker}\alpha) \Rightarrow \exists a \in \text{Ker}\alpha, \gamma(a) = c \Rightarrow \alpha(a) = 0$ và $\delta(c) = \delta(\gamma(a)) = \beta(\alpha(a)) = \beta(0) = 0 \Rightarrow c \in \text{Ker}\delta$. Do đó $\gamma(\text{Ker}\alpha) \subset \text{Ker}\delta$.

Vậy $\text{Ker}\delta = \gamma(\text{Ker}\alpha)$.

26. a) $\forall x \in A$, đặt $y = \varphi(x)$ và $z = x - y$. Khi đó $x = y + z$ với $y \in \text{Im}\varphi$ và $z \in \text{Ker}\varphi$ do $\varphi(z) = \varphi(x) - \varphi(y) = \varphi(x) - \varphi(\varphi(x)) = \varphi(x) - \varphi(x) = 0$. Do đó $A = \text{Im}\varphi + \text{Ker}\varphi$.

$x \in \text{Im}\varphi \cap \text{Ker}\varphi \Rightarrow \exists u \in A, \varphi(u) = x$ và $\varphi(x) = 0 \Rightarrow x = \varphi(u) = \varphi(\varphi(u)) = \varphi(x) = 0$. Do đó $\text{Im}\varphi \cap \text{Ker}\varphi = \{0\}$.

Vậy $A = \text{Im}\varphi \oplus \text{Ker}\varphi$.

b) $\forall x \in B$, $\psi(x) \in C$, nên $\exists u \in A$ sao cho $\psi \circ \varphi(u) = \psi(x)$. Khi đó $y = \varphi(u) \in \text{Im}\varphi$ và với $z = x - y$ ta có $\psi(z) = \psi(x) - \psi(y) = 0$ hay $z \in \text{Ker}\psi$. Vậy $\forall x \in B$, $x = y + z$ với $y \in \text{Im}\varphi$ và $z \in \text{Ker}\psi$ hay $B = \text{Im}\varphi + \text{Ker}\psi$.

$x \in \text{Im}\varphi \cap \text{Ker}\psi \Rightarrow \exists u \in A, x = \varphi(u)$ và $\psi \circ \varphi(u) = \psi(x) = 0 \Rightarrow u = 0$ và $x = \varphi(0) = 0$. Vậy $\text{Im}\varphi \cap \text{Ker}\psi = \{0\}$. Do đó $B = \text{Im}\varphi \oplus \text{Ker}\psi$.

27. a) Xét hai phép chiếu $p : M \times M' \rightarrow M$ và $q : M \times M' \rightarrow M'$ cho bởi $p(x, y) = x$, $q(x, y) = y$, ta có p và q là hai đồng cấu R -môđun. Xét ánh xạ

$$\begin{aligned} \varphi : \text{Hom}_R(N, M \times M') &\longrightarrow \text{Hom}_R(N, M) \times \text{Hom}_R(N, M') \\ f &\mapsto (p \circ f, q \circ f). \end{aligned}$$

MATH-EDUCARE

Khi đó φ là một đồng cấu R -môđun. Thật vậy,

$\forall f, g \in Hom_R(N, M \times M')$, $\forall a, b \in R$,

$$\begin{aligned}\varphi(af + bg) &= (p \circ (af + bg), q \circ (af + bg)) \\ &= (a(p \circ f) + b(p \circ g), a(q \circ f) + b(q \circ g)) \\ &= a(p \circ f, q \circ f) + b(p \circ g, q \circ g).\end{aligned}$$

φ là đơn cấu vì $(p \circ f, q \circ f) = 0$ kéo theo $f = 0$ hay $Ker\varphi = \{0\}$.

φ là toàn cấu vì $\forall (g, h) \in Hom_R(N, M) \times Hom_R(N, M')$,

$\exists f \in Hom_R(N, M \times M')$ xác định bởi $f(z) = (g(z), h(z))$ sao cho $\varphi(f) = (g, h)$.

Vậy φ là một đồng cấu.

b) Xét hai phép nhúng $i : M \longrightarrow M \times M'$ và $j : M' \longrightarrow M \times M'$ cho bởi $i(x) = (x, 0)$, $j(y) = (0, y)$, ta có i và j là hai đồng cấu R -môđun. Xét ánh xạ

$$\begin{aligned}\varphi : Hom_R(M \times M', N) &\longrightarrow Hom_R(M, N) \times Hom_R(M', N) \\ f &\mapsto (f \circ i, f \circ j).\end{aligned}$$

Khi đó φ là một đồng cấu R -môđun. Thật vậy,

$\forall f, g \in Hom_R(M \times M', N)$, $\forall a, b \in R$,

$$\begin{aligned}\varphi(af + bg) &= ((af + bg) \circ i, (af + bg) \circ j) \\ &= (a(f \circ i) + b(g \circ i), a(f \circ j) + b(g \circ j)) \\ &= a(f \circ i, f \circ j) + b(g \circ i, g \circ j).\end{aligned}$$

φ là đơn cấu vì $(f \circ i, f \circ j) = 0$ kéo theo $f = 0$ hay $Ker\varphi = \{0\}$.

φ là toàn cấu vì $\forall (g, h) \in Hom_R(M, N) \times Hom_R(M', N)$, $\exists f \in Hom_R(M \times M', N)$ xác định bởi $f(x, y) = g(x) + h(y)$ sao cho $\varphi(f) = (g, h)$.

Vậy φ là một đồng cấu.

28. Do g là toàn cấu nên $\forall c \in C$, $\exists b \in B$, $g(b) = c$. Khi đó ta có ánh xạ $k : C \longrightarrow D$ xác định bởi $k(c) = h(b)$; thật vậy, nếu $\exists b, b' \in B$ sao cho $g(b) = g(b') = c$ thì $b - b' \in Ker g = Im f$ do đó $\exists a \in A$ sao cho $b - b' = f(a)$ và $h(b) - h(b') = h(b - b') = h(f(a)) = 0$ hay $h(b) = h(b')$.

$\forall c, c' \in C$, $\forall \alpha, \alpha' \in R$, $\exists b, b' \in B$ sao cho $g(b) = c$, $g(b') = c'$, nên $g(\alpha b + \alpha' b') = \alpha c + \alpha' c'$. Khi đó $k(\alpha c + \alpha' c') = h(\alpha b + \alpha' b') = \alpha h(b) + \alpha' h(b') = \alpha k(c) + \alpha k(c')$, do đó k là một đồng cấu R -môđun.

Từ định nghĩa của k , ta có $k \circ g = h$ và nếu tồn tại $k' : C \rightarrow D$ sao cho $k' \circ g = h$ thì $k = k'$.

29. $\forall d \in D, g(h(d)) = 0$, nên $h(d) \in Kerg = Imf$, do đó $\exists a \in A$ sao cho $f(a) = h(d)$. Xét phép tương ứng $k : D \rightarrow A$ cho bởi $k(d) = a$ với $f(a) = h(d)$. k là một ánh xạ vì nếu $\exists a, a'$ sao cho $f(a) = f(a') = h(d)$ thì $a = a'$ (do f là đơn cấu).

$\forall d, d' \in D, \forall \lambda, \lambda' \in R, \exists a, a' \in A$ sao cho $a = a', k(d') = a'$ với $f(a) = h(d), f(a') = h(d')$, nên $f(\lambda a + \lambda' a') = h(\lambda d + \lambda' d')$. Khi đó $k(\lambda d + \lambda' d') = \lambda a + \lambda' a' = \lambda k(d) + \lambda' k(d')$, do đó k là một đồng cấu R -môđun.

Từ định nghĩa của k , ta có $f \circ k = h$ và nếu tồn tại $k' : D \rightarrow A$ sao cho $f \circ k' = h$ thì $k = k'$.

30. Áp dụng Bài 26 với $h = g' \circ \beta : B \rightarrow C'$ thoả mãn $h \circ f = g' \circ \beta \circ f = g' \circ f' \circ \alpha = 0$, tồn tại một đồng cấu R -môđun duy nhất $\gamma : C \rightarrow C$ thoả mãn $\gamma \circ g = h = g' \circ \beta$.

31. Áp dụng Bài 27 với $h = \beta \circ f : A \rightarrow B'$ thoả mãn $g' \circ h = g' \circ \beta \circ f = \gamma \circ g \circ f = 0$, tồn tại một đồng cấu R -môđun duy nhất $\alpha : A \rightarrow A'$ thoả mãn $f' \circ \alpha = h = \beta \circ f$.

32. a)

$$\begin{aligned} b' \in Im\beta &\Rightarrow \exists b \in B, \beta(b) = b' \Rightarrow g'(b') = g'(\beta(b)) = \gamma(g(b)) \in Im\gamma \\ &\Rightarrow b' \in g'^{-1}(Im\gamma) \end{aligned}$$

Do đó $Im\beta \subset g'^{-1}(Im\gamma)$.

$$\begin{aligned} b' \in g'^{-1}(Im\gamma) &\Rightarrow g'(b') \in Im\gamma \Rightarrow \exists c \in C, \gamma(c) = g'(b') \\ &\Rightarrow \delta(h(c)) = h'(\gamma(c)) = h'(g'(b')) = 0 \\ &\Rightarrow h(c) = 0 \text{ (vì } \delta \text{ là một đơn cấu)} \Rightarrow c \in Kerh = Img \\ &\Rightarrow \exists b \in B, g(b) = c \Rightarrow g'(b' - \beta(b)) = g'(b') - g'(\beta(b)) = \\ &\qquad\qquad\qquad \gamma(c) - \gamma(g(b)) = \gamma(c) - \gamma(c) = 0 \\ &\Rightarrow b' - \beta(b) \in Kerg' = Imf' \\ &\Rightarrow \exists a' \in A', f'(a') = b' - \beta(b) \text{ và } \exists a \in A, \alpha(a) = a' \\ &\qquad\qquad\qquad \text{(vì } \alpha \text{ là một toàn cấu)} \\ &\Rightarrow b' = (b' - \beta(b)) + \beta(b) = f'(a') + \beta(b) \\ &\qquad\qquad\qquad = f'(\alpha(a)) + \beta(b) = \beta(f(a)) + \beta(b) \\ &\qquad\qquad\qquad = \beta(f(a) + b) \in Im\beta \end{aligned}$$

Do đó $g'^{-1}(Im\gamma) \subset Im\beta$.

Vậy $Im\beta = g'^{-1}(Im\gamma)$.

b)

$c \in Ker\gamma \Rightarrow \gamma(c) = 0$ và $\delta(h(c)) = h'(\gamma(c)) = h'(0) = 0$
 $\Rightarrow h(c) = 0$ (vì δ là một đơn cấu) $\Rightarrow c \in Kerh = Img$
 $\Rightarrow \exists b \in B, g(b) = c \Rightarrow g'(\beta(b)) = \gamma(g(b)) = \gamma(c) = 0$
 $\Rightarrow \beta(b) \in Kerg' = Imf' \Rightarrow \exists a' \in A', f'(a') = \beta(b)$
 $\Rightarrow \exists a \in A, \alpha(a) = a'$ (vì α là một toàn cấu)
 $\Rightarrow \beta(b - f(a)) = \beta(b) - \beta(f(a)) = \beta(b) - f'(\alpha(a)) = 0$
 $\Rightarrow b - f(a) \in Ker\beta$ và $g(b - f(a)) = g(b) - g(f(a)) = c - 0 = c$
 $\Rightarrow c \in g(Ker\beta)$

Do đó $Ker\gamma \subset g(Ker\beta)$.

$c \in g(Ker\beta) \Rightarrow \exists b \in Ker\beta, g(b) = c$
 $\Rightarrow \gamma(c) = \gamma(g(b)) = g'(\beta(b)) = g'(0) = 0 \Rightarrow c \in Ker\gamma$

Do đó $g(Ker\beta) \subset Ker\gamma$.

Vậy $Ker\gamma = g(Ker\beta)$.

33. a) Áp dụng Bài 22 cho biểu đồ sau với 0 là toàn cấu và γ là đơn cấu:

$$\begin{array}{ccccccc} 0 & \xrightarrow{0} & A & \xrightarrow{f} & B & \xrightarrow{g} & C \\ 0 \downarrow & & \alpha \downarrow & & \beta \downarrow & & \gamma \downarrow \\ 0 & \xrightarrow{0} & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' \end{array}$$

ta có $Ker\beta = f(Ker\alpha) = f(0) = 0$ (do α là đơn cấu), do đó β là đơn cấu.

b) Áp dụng Bài 22 cho biểu đồ sau với α là toàn cấu và 0 là đơn cấu:

$$\begin{array}{ccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{0} & 0 \\ \alpha \downarrow & & \beta \downarrow & & \gamma \downarrow & & 0 \downarrow \\ A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \xrightarrow{0} & 0 \end{array}$$

ta có $Im\beta = g'^{-1}(Im\gamma) = g'^{-1}(C') = B'$ (do γ toàn cấu), do đó β là toàn cấu.

34. $\forall c \in C$, do φ là toàn cấu, $\exists a \in A$ sao cho $\varphi(a) = c$ và ta có $\alpha(a) \in B$. Xét phép tương ứng $\lambda : C \rightarrow B$ cho bởi $\lambda(c) = \alpha(a)$ sao cho $\varphi(a) = c$.

Nếu $\exists a, a' \in A$ sao cho $\varphi(a) = \varphi(a') = c$ thì $a - a' \in Ker\varphi$, nên $a - a' \in Ker\alpha$, do đó $\alpha(a) = \alpha(a')$. Điều này cho biết λ là một ánh xạ.

MATH-EDUCARE

$\forall a \in A$, đặt $c = \varphi(a)$, ta có $\lambda \circ \varphi(a) = \lambda(c) = \alpha(a)$, do đó $\lambda \circ \varphi = \alpha$

$$Im\alpha = \lambda \circ \varphi(A) = \lambda(\varphi(A)) = \lambda(C) = Im\lambda.$$

Cho λ là một đơn cầu. Khi đó $\forall a \in Ker\alpha$, ta có $\lambda(\varphi(a)) = \lambda \circ \varphi(a) = \alpha(a) = 0$, nên $\varphi(a) = 0$ hay $a \in Ker\varphi$. Do đó $Ker\alpha \subset Ker\varphi$. Vậy $Ker\varphi = Ker\alpha$.

cho $Ker\varphi = Ker\alpha$. Khi đó $\forall c \in Ker\lambda$, ta có $\lambda(c) = 0$ và $\exists a \in X$ sao cho $\varphi(a) = c$, nên $\alpha(a) = \lambda(\varphi(a)) = \lambda(c) = 0$ hay $a \in Ker\alpha = Ker\varphi$, do đó $c = \varphi(a) = 0$. Vậy $Ker\lambda = \{0\}$ hay λ là một đơn cầu.

35. a) Ta chỉ cần chứng minh $\varphi(Ker\alpha) \subset Ker\beta$ và $\psi(Ker\beta) \subset Ker\gamma$

$$y \in \varphi(Ker\alpha) \Rightarrow \exists x \in Ker\alpha, y = \varphi(x)$$

$$\Rightarrow \beta(y) = \beta(\varphi(x)) = \varphi'(\alpha(x)) = \varphi'(0) = 0$$

$$\Rightarrow y \in Ker\beta$$

Do đó $\varphi(Ker\alpha) \subset Ker\beta$. Tương tự $\psi(Ker\beta) \subset Ker\gamma$.

b) Ta chỉ cần chứng minh $\varphi'(Im\alpha) \subset Im\beta$ và $\psi'(Im\beta) \subset Im\gamma$.

$$y' \in \varphi'(Im\alpha) \Rightarrow \exists x' \in Im\alpha, y' = \varphi(x')$$

$$\Rightarrow \exists x \in X, \alpha(x) = x', y' = \varphi'(x')$$

$$\Rightarrow y' = \varphi'(\alpha(x)) = \beta(\varphi(x)) \in Im\beta$$

Do đó $\varphi'(Im\alpha) \subset Im\beta$. Tương tự $\psi'(Im\beta) \subset Im\gamma$.

c) Đặt $\varphi_1 = \varphi|_{Ker\alpha}$ và $\psi_1 = \psi|_{Ker\beta}$. Do $\psi \circ \varphi = 0$, ta có $\psi_1 \circ \varphi_1 = 0$ hay $Im\varphi_1 \subset Ker\psi_1$.

$$y \in Ker\psi_1 \Rightarrow y \in Ker\psi \text{ và } y \in Ker\beta \Rightarrow y \in Im\varphi \text{ và } y \in Ker\beta$$

$$\Rightarrow \exists x \in X, y = \varphi(x) \text{ và } \beta(y) = 0$$

$$\Rightarrow \varphi'(\alpha(x)) = \beta(\varphi(x)) = \beta(y) = 0$$

$$\Rightarrow \alpha(x) = 0 \text{ (vì } \varphi' \text{ là đơn cầu)} \Rightarrow x \in Ker\alpha$$

$$\Rightarrow y \in Im\varphi_1$$

Do đó $Ker\psi_1 \subset Im\varphi_1$. Vậy $Im\varphi_1 = Ker\psi_1$ hay (1) là khớp. Đặt $\varphi'_1 = \varphi|_{Im\alpha}$ và $\psi'_1 = \psi|_{Im\beta}$. Do $\psi' \circ \varphi' = 0$, ta có $\psi'_1 \circ \varphi'_1 = 0$ hay $Im\varphi'_1 \subset Ker\psi'_1$.

$$y' \in Ker\psi'_1 \Rightarrow y' \in Ker\psi' \text{ và } y' \in Im\beta$$

$$\Rightarrow y' \in Im\varphi' \text{ và } \exists y \in Y, y' = \beta(y)$$

$$\Rightarrow \exists x \in X, y = \varphi(x) \text{ và } y' = \beta(y) \text{ (vì } \varphi \text{ là toàn cầu)}$$

$$\Rightarrow y' = \beta(\varphi(x)) = \varphi'(\alpha(x)) \in Im\varphi'_1$$

Do đó $Ker\psi'_1 \subset Im\varphi'_1$. Vậy $Im\varphi'_1 = Ker\psi'_1$ hay (2) là khớp.

MATH-EDUCARE
TÀI LIỆU THAM KHẢO

- [1] *G. Birkhoff và S. MacLane*, Tổng quan về đại số hiện đại (Bản dịch tiếng Việt), NXB ĐH & THCN, Hà Nội, 1979.
- [2] *Nguyễn Gia Định*, Giáo trình Toán cao cấp 1 (Phần Đại số), NXB Giáo dục, Hà Nội, 2005.
- [3] *Nguyễn Gia Định*, Bài tập Đại số (Tập 1), NXB Giáo dục, Hà Nội, 2004.
- [4] *Nguyễn Gia Định*, Cơ sở Toán học, NXB Đại học Huế, 2008.
- [5] *Bùi Duy Hiền*, Bài tập Đại số đại cương, NXB Giáo dục, Hà Nội, 2001.
- [6] *Trần Diên Hiển, Nguyễn Văn Ngọc*, Giáo trình Toán cao cấp I, NXB Giáo dục, Hà Nội, 1997.
- [7] *Nguyễn Hữu Việt Hưng*, Đại số đại cương, NXB Giáo dục, Hà Nội, 1993.
- [8] *Jean-Marie Monier*, Đại số 1, Giáo trình Toán - Tập 5 (Bản dịch tiếng Việt), NXB Giáo dục, 2000.
- [9] *Ngô Thế Phiệt*, Giáo trình đại số (Tập 1), Trường Đại học Tổng hợp Huế, Huế, 1977.
- [10] *Helena Rasiowa*, Cơ sở của toán học hiện đại (Bản dịch tiếng Việt), NXB Khoa học và Kỹ thuật, Hà Nội, 1978.
- [11] *Kenneth H. Rosen*, Toán học rời rạc ứng dụng trong tin học (Bản dịch tiếng Việt), NXB Khoa học và Kỹ thuật, Hà Nội, 1997.
- [12] *Hoàng Xuân Sính*, Đại số đại cương, NXB Giáo dục, Hà Nội, 1995.