

Morphisms, Rings and Fields

S. D. Joshi, Dandli
CSE-AP 1751007

1. Show that the groups $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$ are not isomorphic.

Soln: $(\mathbb{Z}, +)$ is a cyclic group. Isomorphic image of a cyclic group must be cyclic. But $(\mathbb{Q}, +)$ is not a cyclic group.

$\therefore (\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$ are not isomorphic.

2. Determine whether the given map ϕ is a homomorphism.

(a) $\phi : \mathbb{R} \rightarrow \mathbb{Z}$ under addition given by $\phi(x) = \text{the greatest integer } \leq x$.

(b) $\phi : \mathbb{R}^+ \rightarrow \mathbb{R}^+$ under multiplication given by $\phi(x) = |x|$.

(c) Let $M_n(\mathbb{R})$ be the additive group of all $n \times n$ matrices with real entries and $\phi(A) = \det(A)$, $A \in M_n(\mathbb{R})$.

Soln: (a) Let $x \in G_1, y \in G_1$. Then $xy \in G_1$.

$$\phi(x) = [x] \quad \phi(y) = [y] \quad \phi(xy) = [xy]$$

We know

$$[xy] \neq [x] + [y] \quad \left[\begin{array}{l} \text{eg: let } x = 2.5 \text{ & } y = 1.5 \\ \text{then } [xy] = 1 \quad [x] = 2 \quad [y] = 1 \\ \therefore [x] + [y] = 3 \neq [xy] \end{array} \right]$$

$$\therefore \phi(xy) \neq \phi(x) + \phi(y)$$

Therefore ϕ is not a homomorphism.

(b) Let $x \in G_1, y \in G_1$. Then $xy \in G_1$.

$$\phi(x) = |x| \quad \phi(y) = |y| \quad \phi(xy) = |xy|$$

We know

$$|xy| = |x||y|$$

$$\therefore \phi(xy) = \phi(x)\phi(y)$$

$\therefore \phi$ is a homomorphism.

(c) Let $x \in G_1, y \in G_1$. Then $xy \in G_1$.

where x, y are $n \times n$ matrices.

$$\phi(x) = \det x \quad \phi(y) = \det y \quad \phi(xy) = \det(xy)$$

But $\det(x+y) \neq \det(x) + \det(y)$

(eg: $x = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, y = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ [$\det(x)=1, \det(y)=1$, $\det(x+y)=0$])

$\therefore \phi(x+y) \neq \phi(x) + \phi(y)$.

$\Rightarrow \phi$ is not a homomorphism.

Prove that \mathbb{Z}_8 is not a homomorphic image of \mathbb{Z}_{15} .

Soln. We know that group $G_1 \& G_2$ is said to be the homomorphic image of G_1' if $\phi(G_1)$ is a divisor of $O(G_1')$.

As we can see that 8 is not a divisor of 15.

So we can clearly say that \mathbb{Z}_8 is not a homomorphic image of \mathbb{Z}_{15} .

5) Prove that the cancellation law holds in a ring R iff R has no divisor of zero.

Soln. Let R be a ring in which cancellation law holds.

Let $a, b \in R$ and $a \cdot b = 0$ where $a \neq 0$.

Then $a \cdot b = 0 = a \cdot 0$

\because The cancellation law holds, $b=0$.

This proves that a is not a left divisor of zero.

Let $a, b \in R$ and $a \cdot b = 0$ where $b \neq 0$.

Then $a \cdot b = 0 = 0 \cdot b$

\therefore The cancellation law holds, $a=0$.

This proves that b is not the right divisor of zero.

Thus R has neither left or right divisor of zero.
Conversely, let R has no divisor of 0. Let $a, b, c \in R$ & $ab=ac$. \therefore at $a(b-c)=0$, $\therefore R$ contains no divisor of 0. $b-c=0 \Rightarrow b=c$.
 \therefore left cancellation law holds in R.

Similar arguments prove that right cancellation law holds. (proved)

6) Show that the ring of matrices $\left\{ \begin{pmatrix} 2a & 0 \\ 0 & 2b \end{pmatrix} : a, b \in \mathbb{Z} \right\}$ contains divisors of 0 and does not contain the unity.

Soln: Let S be the ring and let $E = \begin{pmatrix} 2x & 0 \\ 0 & 2y \end{pmatrix} \in S$ be the unity.
Then $AE = EA = A$ & $A \in S$.

Let $A = \begin{pmatrix} 2a & 0 \\ 0 & 2b \end{pmatrix}$. Then $AE = A$ implies

$$\begin{pmatrix} 2a & 0 \\ 0 & 2b \end{pmatrix} \begin{pmatrix} 2x & 0 \\ 0 & 2y \end{pmatrix} = \begin{pmatrix} 2a & 0 \\ 0 & 2b \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 4ax & 0 \\ 0 & 4by \end{pmatrix} = \begin{pmatrix} 2a & 0 \\ 0 & 2b \end{pmatrix}$$

$$\Rightarrow 4ax = 2a \text{ & } 4by = 2b$$

$\therefore a = \frac{1}{2}$ & $y = \frac{1}{2}$ & $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ not possible as $a, y \in \mathbb{Z}$.

So S does not contain unity.

$\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ are non zero elements of S &

$\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ shows that S contains divisors of 0.

7) Examine the ring of matrices $\left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$ contains divisors of zero.

Let S be the ring and $A = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ be a non zero element of S . Then $a, b \in \mathbb{R}$ and $(a, b) \neq (0, 0)$.

Let $AB = 0$, where $B = \begin{pmatrix} p & q \\ 2q & p \end{pmatrix}$.

$$\text{This (1) gives } ap + 2bq = 0$$

$$bp + aq = 0$$

This is a homogeneous system of equations giving non zero solutions for p, q if $\begin{vmatrix} a & 2b \\ b & a \end{vmatrix} = 0$ i.e. if $a^2 - 2b^2 = 0$

Now from (2) we can get non zero values of a, b

e.g. $a = \sqrt{2}$ & $b = 1$. In this case a non zero matrix B exists such that $AB = 0$

$\therefore S$ contains divisors of zero.

$$\text{eg: } \begin{pmatrix} \sqrt{2} & 1 \\ -\sqrt{2} & \sqrt{2} \end{pmatrix} \begin{pmatrix} -\sqrt{2} & 1 \\ 2 & -\sqrt{2} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Q) Prove that the ring $\mathbb{Z}[x]$, the ring of all polynomials with integer coefficients is an integral domain.

Soln. The ring $\mathbb{Z}[x]$ is a commutative ring with unity, the constant polynomial 1 being the identity element.

The zero element in the ring is the constant polynomial 0.

Let $f(x), g(x)$ be non zero polynomials in $\mathbb{Z}[x]$ of degrees m, n respectively

$$\text{let } f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_m x^m \quad \& \quad g(x) = b_0 + b_1 x + b_2 x^2 + \dots + b_n x^n \text{ where } a_m \neq 0 \quad \& \quad b_n \neq 0.$$

Then $f(x)g(x)$ is a polynomial in $\mathbb{Z}[x]$ with a non zero polynomial term $a_m b_n x^{m+n}$ since $a_m b_n \neq 0$ and therefore $f(x)g(x)$ is a non zero polynomial in $\mathbb{Z}[x]$. Thus $\mathbb{Z}[x]$ has no divisors of zero and therefore it is an integral domain.

a) Prove that the ring of matrices $\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$ is a field.

Soln. Let $S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$, $(S, +, \cdot)$ is a ring with unity

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ being the unity.

Let $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, B = \begin{pmatrix} p & q \\ -q & p \end{pmatrix} \in S$. Then

$$A \cdot B = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} p & q \\ -q & p \end{pmatrix} = \begin{pmatrix} ap - bq & aq + bp \\ -bp - aq & -bq + ap \end{pmatrix}$$

$$B \cdot A = \begin{pmatrix} p & q \\ -q & p \end{pmatrix} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} ap - bq & aq + bp \\ -bp - aq & -bq + ap \end{pmatrix}$$

Therefore $AB = BA \quad \forall A, B \in S$.

Hence $(S, +, \cdot)$ is a commutative ring with unity.

Let $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ be a non zero element of S .

Then $(a, b) \neq (0, 0)$ & $\det A = a^2 + b^2 \neq 0$.

Hence A^{-1} exists & $A^{-1} = \frac{1}{a^2 + b^2} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in S$

∴ Every non zero element of a ring is a unit.

Hence $(S, +, \cdot)$ is a field.

10)

Prove that the ring of matrices $\left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} : a, b \in \mathbb{Q} \right\}$ is a field.

Soln:

Let $S = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} : a, b \in \mathbb{Q} \right\}$, $(S, +, \cdot)$ is a ring with unity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ being the unity.

Let $A = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$, $B = \begin{pmatrix} p & q \\ 2q & p \end{pmatrix} \in S$. Then

$$A \cdot B = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \begin{pmatrix} p & q \\ 2q & p \end{pmatrix} = \begin{pmatrix} ap + 2bq & aq + bp \\ 2bp + 2aq & 2bq + ap \end{pmatrix}$$

$$B \cdot A = \begin{pmatrix} p & q \\ 2q & p \end{pmatrix} \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} = \begin{pmatrix} ap + 2bq & aq + bp \\ 2bp + 2aq & 2bq + ap \end{pmatrix}$$

∴ $AB = BA \neq A, B \in S$.

∴ $(S, +, \cdot)$ is a commutative ring with unity.

Let $A = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ be a non zero element of S . Then $(a, b) \neq (0, 0)$

and a, b are rational.

$$\det A = a^2 - 2b^2 \neq 0$$
 as $(a, b) \neq (0, 0)$

Hence A^{-1} exists and $A^{-1} = \frac{1}{a^2 - 2b^2} \begin{pmatrix} a & -b \\ -2b & a \end{pmatrix} \in S$.

∴ Each ^{non zero} element of S is a unit.

∴ $(S, +, \cdot)$ is a field.

ii) Examine the sum of matrices $\{(a \ b) : a, b \in R\}$ if R is a field.
 Soln. Let $S = \{(a \ b) : a, b \in R\}$. S is a commutative ring with unity $(1 \ 0)$.

Let $A = (a \ b)$ be a non zero element of S . Then $(a, b) \neq (0, 0)$. A^{-1} exists only if $\det A \neq 0$.

Now $\det A = a^2 - 2b^2$. There exist non zero real no's for which $\det A = 0$ eg: $a = \sqrt{2}, b = 1$.

\therefore Non zero matrix $(\sqrt{2} \ 1)$ has no inverse.

$\therefore (S, +, \cdot)$ is not a field.

12) Prove that the set S of matrices $\{(a \ 0 \ 0 \ c) : a, b, c \in \mathbb{Z}\}$ is a subring of $M_2(\mathbb{Z})$.

Now when $a, b, c = 0$ $(0 \ 0 \ 0 \ 0) \in S \therefore S \neq \emptyset$

Let $A = (a \ 0 \ b \ c)$, $B = (p \ 0 \ q \ r)$

$$A - B = (a-p \ 0 \ b-q \ c-r) \in S$$

$$A \cdot S = (ap \ 0 \ bp+cq \ cr) \in S.$$

$\therefore S$ is a subring of $M_2(\mathbb{Z})$.

13) Prove that $(\mathbb{Z}_{\text{primes}}, +, \cdot)$ is an integral domain iff n is prime.

Let n be a composite number.

$$n = pq, 1 < p < n, 1 < q < n$$

$\therefore n = p \cdot q = \bar{0} \Rightarrow$ Existence of divisors of 0.

\therefore It is a contradiction

$\therefore n$ is prime.

Let n be a prime no:
 $(\mathbb{Z}_n, +, \cdot) \rightarrow$ commutative ring with unity.
 Let $m \in \mathbb{Z}_n$ & $\gcd(m, n) = 1$.

$$\Rightarrow mn \text{ & } m^2 \equiv 1 \pmod{n}$$

$$\Rightarrow n \mid m^2 - 1$$

$$m^2 - 1 = 0 \Rightarrow m \bar{u} = \bar{1}$$

$$\text{If } u \mid n \quad u = nq + r$$

$$\Rightarrow \bar{u} = \bar{r}$$

$$\therefore \bar{m} \cdot \bar{r} = \bar{1} = \bar{r} \cdot \bar{m}$$

(Now) Every element of \mathbb{Z}_n is an unit.

14) Prove that the ring $\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$, the ring of Gaussian integers, is an integral domain.

Sol: The ring of Gaussian integers is a commutative ring with unity. 1 being the unit ($1+0i$)

$$\text{Let } (a+bi)(c+di) = 0$$

$$\text{Let } a+bi \neq 0 \text{ Then } (a, b) \neq (0, 0)$$

$$(a+bi)(c+di) = 0 \Rightarrow a+bi=0 \Rightarrow c+di=0$$

$$\text{WITA } a+bi \neq 0 \Rightarrow c+di=0$$

$$\text{gives } ac - bd = 0, ad + bc = 0$$

This is a homogeneous system of eqns in a, b having non zero solutions. Therefore the coefficient of det of the system, $c^2 + d^2$ is 0. This gives $c=0$ & $d=0$.

Thus $(a+bi)(c+di)$ with $a+bi \neq 0 \Rightarrow c+di=0$.

\therefore It contains no divisor of 0. Hence it is an integral domain.

15) Prove that \mathbb{Z}_{11} , the ring of all integers modulo 11 is a field. State any theorem that you use. Find the multiplicative inverses of the non-zero elements of \mathbb{Z}_{11} .

Sol^m. As we know that $(\mathbb{Z}_m, +, \cdot)$ is an integral domain if m is prime.

Here we can see that $m=11$ is prime.

$\therefore (\mathbb{Z}_{11}, +, \cdot)$ is an integral domain.

Also we know that any finite integral domain is a field.

$\therefore (\mathbb{Z}_{11}, +, \cdot)$ is a field.

We know m is a multiplicative inverse if $(m, 11)=1$.

$$\therefore m = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$$

16) Let R be a ring. The centre of R is the set $\{x \in R : ax = xa\}$ for all $a \in R$. Prove that centre of a ring is subring.

Let $Z(R) = \{x \in R : ax = xa\}$

Aim : to show,
 $a(x-y) = (x-y)a$
 $a(xy) = x(a(y)a)$.

Let $x, y \in Z(R)$

$$\therefore ax = xa \text{ & } ay = ya.$$

$$a(xy) = (ax)y = (xa)y = x(ay) = (xy)a \quad \text{L (1)}$$

$$\begin{aligned} \text{Now } a(x-y) &= ax - ay = xa - ya \\ &= (x-y)a. \quad \text{— (2)} \end{aligned}$$

From (1) & (2) we see that centre of a ring is subring.

17) In a ring $(\mathbb{Z}_m, +, \cdot)$, $[m]$ is a unit if and only if $\gcd(m, n) = 1$.

Let \bar{m} be the unit of $(\mathbb{Z}_m, +, \cdot)$. Then $\exists \bar{n} \in \mathbb{Z}_m$ s.t.

$$\bar{m} \cdot \bar{n} = 1 \Rightarrow \bar{m} \cdot \bar{n} - 1 = \bar{0}$$

$$\begin{aligned} &\Rightarrow \bar{m}\bar{n} - 1 = \bar{0} \\ &\Rightarrow m|\bar{m}\bar{n} - 1 \end{aligned}$$

$$\Rightarrow mu - 1 = nv$$

$$\Rightarrow mu - nv = 1$$

$$\Rightarrow \gcd(m, n) = 1.$$

Conversely let $\gcd(m, n) = 1$

$$\Rightarrow mu + nv = 1$$

$$\Rightarrow n | mu - 1 \Rightarrow \overline{m}u = 1$$

If $n | m$ by division algorithm,

$$u = mq + r$$

$$\text{Now } \overline{m} \cdot \overline{u} = 1 \Rightarrow \overline{m} \cdot \overline{r} = 1 = \overline{r} \cdot \overline{m}$$

Hence \overline{m} is a unit in \mathbb{Z}_n .

- 18) In a ring R with unity $(xy)^2 = x^2y^2 \forall x, y \in R$, then show that R is commutative.

Since the unity of ring $1 \in R$, so for all $x, y \in R$

$$[x(y+1)]^2 = x^2(y+1)^2, \text{ by given condition.}$$

$$\Rightarrow [x(y+1)][x(y+1)] = x^2(y+1)(y+1)$$

$$\Rightarrow (xy+x)(xy+x) = x^2[y(y+1)+1(y+1)]$$

$$\Rightarrow (xy)^2 + xyx + xxy + x^2 = x^2[y^2 + y + y + 1]$$

$$\Rightarrow (xy)^2 + xyx + xxy + x^2 = x^2y^2 + x^2y + x^2y + x^2$$

$$\Rightarrow x^2y^2 + xyx + xxy + x^2 = x^2y^2 + x^2y + x^2y + x^2$$

$$\Rightarrow xyx + x^2y = x^2y + x^2y$$

$$\Rightarrow xyx = x^2y$$

Replacing xy by $x+1$ we get

$$(x+1)y(x+1) = (x+1)^2y.$$

$$\Rightarrow (xy+y)(x+1) = (x+1)(x+1)y.$$

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

$$\Rightarrow x^2y + xyx + xxy + y = x^2y + xy + xxy + y$$

$$\Rightarrow yx + xy = xy + xy$$

$$\Rightarrow yx = xy \text{ (proved)}$$

1a) For a field F , prove that $a^2 = b^2$ implies either $a=b$ or $a=-b$ $\forall a, b \in F$.

Soln. Now $(a-b)(a+b) = (a-b) \cdot a + (a-b) \cdot b$
By right Distributive law

$$\begin{aligned} &= a \cdot a - b \cdot a + a \cdot b - b \cdot b \\ &= a^2 - a \cdot b + a \cdot b - b^2 [\because a \cdot b = b \cdot a \forall a, b \in F] \\ &= a^2 - b^2 = a^2 - a^2 [\because a^2 = b^2] \\ &= 0. \end{aligned}$$

Either $a-b=0$ or $a+b=0$

i.e. either $a=b$ or $a=-b$.

2b) Find all the solutions of the equation $x^2 + x - 6 = 0$ in \mathbb{Z}_{11} by factoring the quadratic polynomial.

Soln. By factorizing we get $(x+3)(x-2)$

For x, y in \mathbb{Z}_{11} we have $x+y=0$ if $x+y$ is a multiple of 11.

\therefore either x is a multiple of 7 or y is a multiple of 7.

The only 2 multiples of 7 in \mathbb{Z}_{11} are either 7 & 0.

$$\text{So } x+3=0 \text{ or } x-2=0$$

$$x=-3 \quad x=2$$

$$\text{or } x=11.$$

$$\& x+3=7 \quad \text{or} \quad x-2=7$$

$$\Rightarrow x=4 \quad \text{or} \quad x=9.$$

\therefore Solutions of x are 2, 4, 9, 11.

21) Find all solutions of the equation $x^3 - 2x^2 - 3x = 0$ in ring \mathbb{Z}_{12} .

Soln. Factorizing we get,

$$x(x+1)(x-3)=0$$

In \mathbb{Z}_{12} , the product of two non zero elements may be 0.

We have to find all elements of \mathbb{Z}_{12} where $x \in \mathbb{Z}_{12} \text{ & } 0 \leq x \leq 11$

Thus zero occur in \mathbb{Z}_{12} when $x = 0, 3, 5, 8, 9, 11$ in

$$x(x+1)(x-3)=0.$$

Solutions of the eqⁿ. $x^3 - 2x^2 - 3x = 0$ in \mathbb{Z}_{12}

is $0, 3, 5, 8, 9, 11$.

22) An element of a ring R is idempotent if $a^2=a$.

a) Show that the set of all idempotent elements of a commutative ring is closed under multiplication.

Let $a \in R$ then $a+a \in R$.

$$(a+a)^2 = a+a$$

$$\Rightarrow (a+a)(a+a) = a+a$$

$$\Rightarrow (a^2 + a^2) + (a^2 + a^2) = a+a$$

$$\Rightarrow a+a + a+a = a+a \quad [\text{As } a^2 = a]$$

$$\Rightarrow a+a=0 \quad [\text{Applying cancellation law}].$$

$$\text{also } b+b=0 \Rightarrow a=b.$$

Now we have to see whether $a+b$ is an idempotent element or not.

$$(a+b)^2 = (a+b)(a+b)$$

$$= a(a+b) + b(a+b)$$

$$= a^2 + ab + ba + b^2$$

$$= a^2 + a^2 + a^2 + b^2 \quad [\text{as } a=b]$$

$$= a+a+a+b \quad [\text{as } a^2 = a, b^2 = b]$$

$$= a+b \quad [\text{as } a+a=0]$$

(proved)

b) Find all idempotents in the ring $\mathbb{Z}_6 \times \mathbb{Z}_{12}$

The idempotents of this ring are the ordered pairs (a, b) such that a is an idempotent of \mathbb{Z}_6 and b is an idempotent of \mathbb{Z}_{12} .

$$\text{Idempotent of } \mathbb{Z}_6 = \{0, 1, 3, 4\}$$

$$\text{Idempotent of } \mathbb{Z}_{12} = \{0, 1, 4, 9\}$$

$$\therefore \text{Idempotent of } \mathbb{Z}_6 \times \mathbb{Z}_{12} = \{0, 1, 3, 4\} \times \{0, 1, 4, 9\}$$

23) Let R be a commutative ring with unity of characteristic 3. Compute and simplify $(a+b)^6$ for $a, b \in R$.

Soln.

$$\begin{aligned} (a+b)^6 &= a^6 + {}^6C_1 a^5 b + {}^6C_2 a^4 b^2 + {}^6C_3 a^3 b^3 + {}^6C_4 a^2 b^4 \\ &\quad + {}^6C_5 a b^5 + b^6 \\ &= a^6 + 6a^5 b + 15a^4 b^2 + 20a^3 b^3 + 15a^2 b^4 + 6ab^5 + b^6 \end{aligned}$$

Given R is of characteristic 3 then

$6a^5 b + 15a^4 b^2 + 15a^2 b^4$ are 0 as they have a factor of 3.

$$\therefore (a+b)^6 = a^6 + 20a^3 b^3 + b^6.$$

24) Prove that intersection of 2 subring is a subring.

Let R be a ring & S, T be 2 subrings of R .

$S \cap T$ is an non empty set as $0 \in S \cap T$.

Case1: Let $S \cap T = \{0\}$. Then $S \cap T$ is a subring of R .

Case2: Let $S \cap T \neq \{0\}$ & let $p \in S \cap T, q \in S \cap T$.

Then $p \in S, q \in S, p \in T, q \in T$.

Since S is a subring of R then $p-q \in S$ & $p+q \in S$

Since T is a subring of R then $p-q \in T$ & $p+q \in T$

Thus $p \in S \cap T, q \in S \cap T \Rightarrow p-q \in S \cap T$
 $p+q \in S \cap T$

$\therefore S \cap T$ is a subring of R .