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

Proof: 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 in S.

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

Then $A, B \in S$ Now $A.B = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}\begin{pmatrix} p & q \\ 2q & p \end{pmatrix} = \begin{pmatrix} ap+2bq & aq+bp \\ 2bp+2aq & 2bq+ap \end{pmatrix}$

and $B.A = \begin{pmatrix} pa+2qb & pb+qa \\ 2qa+2pb & 2qb+pa \end{pmatrix}$. So, $A.B = B.A$ for all $A, B \in S$

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

Let $A = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ be a non-zero element of S. Then at least one of a and b should be non-zero and a and b are rational. Now $\det A = a^2 - 2b^2 \neq 0$, since at least one of a and b is non-zero and a and b are rational numbers. Hence A^{-1} exists and

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

So, each non-zero element of S is a unit.

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

Exercise: 1. Prove that the set of matrices $\left\{\begin{pmatrix} a & b \\ 3b & a \end{pmatrix} : a, b \in \mathbb{Q}\right\}$ forms a field under matrix addition and matrix multiplication.

Theorem 6 Let S and T be two subrings of a ring R. Then $S \cap T$ is a subring of R.

Proof: $S \cap T$ is non-empty as $0 \in S \cap T$.

Let $p, q \in S \cap T \Rightarrow p, q \in S$ and $p, q \in T$

$\Rightarrow p - q \in S$ and $p \cdot q \in S$ as S is a subring of R

and $p - q \in T$ and $p \cdot q \in T$ as T is a subring of R

So, $p - q \in S \cap T$ and $p \cdot q \in S \cap T$. So, $S \cap T$ is a subring of R

Some examples : 1. Find all the subrings of $(\mathbb{Z}, +, \cdot)$

Solution: Let $(S, +, \cdot)$ be a subring of $(\mathbb{Z}, +, \cdot)$. Then $(S, +)$ must be a subgroup of $(\mathbb{Z}, +)$. But all the subgroups of the group $(\mathbb{Z}, +)$ are the groups $(m\mathbb{Z}, +)$ where m is an integer.

Let us examine if $(m\mathbb{Z}, +, \cdot)$ is a subring of the ring $(\mathbb{Z}, +, \cdot)$

Case I $m = 0$. In this case $(m\mathbb{Z}, +, \cdot)$ reduces to the trivial ring $\{0\}$ and it is a subring.

Case 2 $m \neq 0$, $m\mathbb{Z}$ is a non-empty subset of $\mathbb{Z}$ (as $0 \in m\mathbb{Z}$)

Let $a \in m\mathbb{Z}$, $b \in m\mathbb{Z}$. Then $a - b \in m\mathbb{Z}$ and $a.b \in m\mathbb{Z}$

So, $(m\mathbb{Z}, +, \cdot)$ is a subring of the ring $(\mathbb{Z}, +, \cdot)$

So, all the subrings of the ring $(\mathbb{Z}, +, \cdot)$ are of $(m\mathbb{Z}, +, \cdot)$, where m is an integer.

2. Show that $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a subfield of $(\mathbb{R}, +, \cdot)$

Proof: $\mathbb{Q}[\sqrt{2}]$ is non-empty, as $0 \in \mathbb{Q}[\sqrt{2}]$

Now, Let $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, $c + d\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. Then $a, b, c, d \in \mathbb{Q}$

Now, $(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ as $a - b, c - d \in \mathbb{Q}$ ... (1)

Let $p + q\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ be a non-zero element of $\mathbb{Q}[\sqrt{2}]$

So, at least one of a and b be non-zero

Now $(p + q\sqrt{2})^{-1} = \frac{p}{p^2 - 2q^2} + \frac{-q\sqrt{2}}{p^2 - 2q^2} \in \mathbb{Q}[\sqrt{2}]$, since $p^2 - 2q^2 \neq 0$

as at least one of p and q is non-zero and p and q are rationals.

Also $(a + b\sqrt{2})(p + q\sqrt{2})^{-1} = \frac{ap - 2bq}{p^2 - 2q^2} + \frac{bp - aq}{p^2 - 2q^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ ... (2)

So, from (1) and (2) it follows that $\mathbb{Q}[\sqrt{2}]$ is a subfield of the field $\mathbb{R}$

Exercise: 1. Prove that the set $S = \{a + b\sqrt{5} : a, b \in \mathbb{Q}\}$ is a subfield of $\mathbb{R}$.

---

vector space over a field

Definition: Let V be a non-empty set and $\oplus$ be a binary operation on V. Let $(F, +, \cdot)$ be a field and let $\odot$ be a mapping from $F \times V$ to V, called scalar ~~multiplication~~ multiplication. If $(c, \alpha) \in F \times V$ then $\odot(c, \alpha)$ is denoted by $c \odot \alpha$. V is said to be a vector space over the field F if the following conditions are satisfied:

V1. $\alpha \oplus \beta \in V$ for all $\alpha, \beta \in V$ (you need not mention it as it is automatically satisfied since $\oplus$ is a binary operation on V)

V2. $\alpha \oplus \beta = \beta \oplus \alpha$ for all $\alpha, \beta \in V$,

V3. $\alpha \oplus (\beta \oplus \gamma) = (\alpha \oplus \beta) \oplus \gamma$ for all $\alpha, \beta, \gamma \in V$,

V4. there exists an element θ in V such that $\alpha \oplus \theta = \theta \oplus \alpha = \alpha$ for all $\alpha \in V$,

V5. for each $\alpha \in V$ there exists an element $-\alpha \in V$ such that $\alpha \oplus (-\alpha) = (-\alpha) \oplus \alpha = \theta$,

V6. $c \odot \alpha \in V$ for all $c \in F$, all $\alpha \in V$ (you also need not mention it as it is automatically satisfied since $\odot$ is a mapping from $F \times V$ to V),

V7. $c \odot (d \odot \alpha) = (c \cdot d) \odot \alpha$ for all $c, d \in F$, all $\alpha \in V$,

V8. $c \odot (\alpha \oplus \beta) = (c \odot \alpha) \oplus (c \odot \beta)$ for all $c \in F$, all $\alpha, \beta \in V$,

V9. $(c + d) \odot \alpha = (c \odot \alpha) \oplus (d \odot \alpha)$ for all $c, d \in F$, all $\alpha \in V$

V10. $1 \odot \alpha = \alpha$ for all α, 1 being the multiplicative identity in F.

The vector space [illegible] is denoted by $(V, F, +, \cdot, \oplus, \odot)$. The elements of V are called vectors and the elements of F are called scalars. F is called the ground field (or the field of scalars) of the vector space.

Four symbols $+, \cdot, \oplus, \odot$ denote four different mappings $+ : F \times F \to F$, $\cdot : F \times F \to F$, $\oplus : V \times V \to V$ and $\odot : F \times V \to V$.

We shall dispense with ⊕ and use only + to denote both types of addition. We shall dispense with ⊙ and . both and denote c.d in F by cd and denote c⊙α in V by cα.

So, a non-empty set V is said to form a vector space over a field F if (i) there is a binary operation + on V, called addition, satisfying the conditions

V1. $\alpha+\beta \in V$ for all $\alpha, \beta \in V$

V2. $\alpha+\beta = \beta+\alpha$ for all $\alpha, \beta \in V$

V3. $\alpha+(\beta+\gamma) = (\alpha+\beta)+\gamma$ for all $\alpha, \beta, \gamma \in V$

V4. there exists an element θ in V such that $\alpha+\theta = \alpha$ for all $\alpha \in V$

V5. For each $\alpha \in V$, there exists an element $-\alpha \in V$ such that $\alpha+(-\alpha) = \theta$

and (ii) there is a mapping from F×V to V, called scalar multiplication, satisfying the conditions

V6. $c\alpha \in V$ for all $c \in F$ and for all $\alpha \in V$

V7. $c(d\alpha) = (cd)\alpha$ for all $c, d \in F$ and all $\alpha \in V$

V8. $c(\alpha+\beta) = c\alpha + c\beta$ for all $c \in F$ and all $\alpha, \beta \in V$

V9. $(c+d)\alpha = c\alpha + d\alpha$ for all $c, d \in F$ and all $\alpha \in V$

V10 $1\alpha = \alpha$ for all α, 1 being the multiplicative identity in F.

In particular, V is said to be real vector space (or complex vector if the field F be the field of real numbers $\mathbb{R}$ (or the field of complex numbers $\mathbb{C}$)

Examples: 1. Real vector space $\mathbb{R}^n$: Let $V = \{(a_1, a_2, \ldots, a_n) : a_i \in \mathbb{R}, i = 1, 2, \ldots, n\}$ Let $\oplus$ be the binary operation on $\mathbb{R}^n$, called 'addition', defined by $(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n)$

$$= (a_1+b_1, a_2+b_2, \ldots, a_n+b_n)$$

and the scalar multiplication defined by

$$c(a_1, a_2, \ldots, a_n) = (ca_1, ca_2, \ldots, ca_n), \quad c \in \mathbb{R}.$$

Then we can check that V1 – V10 are satisfied. Therefore V is a real vector space and is denoted by $\mathbb{R}^n$. $(0, 0, \ldots, 0)$ is the null vector θ in $\mathbb{R}^n$. In a similar manner, $\mathbb{R}^1, \mathbb{R}^2, \mathbb{R}^3, \mathbb{R}^4, \ldots$ are defined.