Problem set 2023
Sebastián Caballero Self Study

Vector Spaces I

Problem 1: Let V and W be vector spaces over a field K. Let $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ be a basis for V and let $\{w_1, w_2, \ldots, w_n\}$ be any vectors in W. There is a unique linear map

$$\phi: \quad V \quad \to \quad W$$

Such that $\phi(v_i) = w_i$ for all $1 \leq i \leq n$

Solution. Since $\mathcal{B}$ is a basis for V, for any element $v \in V$ there are $a_1, a_2, \ldots, a_n \in K$ such that:

$$v = a_1v_1 + a_2v_2 + \cdots + a_nv_n$$

so if we define ϕ such that $\phi(v_i) = w_i$ then for any vector v we would have:

$$\begin{aligned} \phi(v) &= a_1\phi(v_1) + a_2\phi(v_2) + \cdots + a_n\phi(a_n) \\ &= a_1w_1 + a_2w_2 + \cdots + a_nw_n \end{aligned}$$

Problem 2: Suppose that V is a finite dimensional vector space. Let $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ be a basis for V then:

- Any set of $w_1, w_2, \ldots, w_n, w_{n+1}$ vectors is linearly dependent
- Any set of $w_1, w_2, \ldots, w_{n-1}$ vectors can't generate V

Solution. For this, we are going to use the facts needed for a basis.

- Let $w_1, w_2, \ldots, w_n, w_{n+1}$ be vectors in V, we can write them in the next way:

$$\begin{aligned} w_1 &= a_{1,1}v_1 + a_{1,2}v_2 + \cdots + a_{1,n}v_n \\ w_2 &= a_{2,1}v_1 + a_{2,2}v_2 + \cdots + a_{2,n}v_n \\ &\cdots\cdots \\ w_n &= a_{n,1}v_1 + a_{n,2}v_2 + \cdots + a_{n,n}v_n \\ w_{n+1} &= a_{n+1,1}v_1 + a_{n+1,2}v_2 + \cdots + a_{n+1,n}v_n \end{aligned}$$

  If there is a w_i such that $w_i = 0$ we are done. Suppose then that this is not true, so for each $1 \leq i \leq n+1$ exists j such that $a_{i,j} \neq 0$. But since there are w_{n+1} there must be i_1, i_2 such that for the same j, we have that $a_{i_1,j} \neq 0 \neq a_{i_2,j}$. So, we can express the vector v_j as:

$$\begin{aligned} v_j &= \frac{w_{i_1}}{a_{i_1,j}} - \frac{a_{i_1,1}v_1 + a_{i_1,2}v_2 + \cdots + a_{i_1,n}v_n}{a_{i_1,j}} \\ v_j &= \frac{w_{i_2}}{a_{i_2,j}} - \frac{a_{i_2,1}v_1 + a_{i_2,2}v_2 + \cdots + a_{i_2,n}v_n}{a_{i_2,j}} \end{aligned}$$

  And so the set is not linearly independent.

- Let $w_1, w_2, \dots, w_{n-1}$ be vectors of V. Suppose that indeed we can generate V with them, so in particular, we can write:

$$\begin{aligned}
v_1 &= a_{1,1}w_1 + a_{1,2}w_2 + \cdots + a_{1,n-1}w_{n-1} \\
v_2 &= a_{2,1}w_1 + a_{2,2}w_2 + \cdots + a_{2,n-1}w_{n-1} \\
\cdots&\cdots \\
v_n &= a_{n,1}w_1 + a_{n,2}w_2 + \cdots + a_{n,n-1}w_{n-1}
\end{aligned}$$

  And since none of them is zero, we can be fure that for each $1 \leq i \leq n$ exists j such that $a_{i,j} \neq 0$. But since there are n vectors in $\mathcal{B}$ and just $n-1$ vectors w_i, there must be i_1, i_2 such that for the same j, we have that $a_{i_1,j} \neq 0 \neq a_{i_2,j}$. So, we can express the vector v_j as:

$$\begin{aligned}
w_j &= \frac{v_{i_1}}{a_{i_1,j}} - \frac{a_{i_1,1}w_1 + a_{i_1,2}w_2 + \cdots + a_{i_1,n}w_n}{a_{i_1,j}} \\
w_j &= \frac{v_{i_2}}{a_{i_2,j}} - \frac{a_{i_2,1}w_1 + a_{i_2,2}w_2 + \cdots + a_{i_2,n}w_n}{a_{i_2,j}}
\end{aligned}$$

  But then this let us generate two different linear combinations within $\mathcal{B}$ that give us the same result, contradicting the linear independency of $\mathcal{B}$.

<u>Problem 3:</u> Let V be a finite vector space. If $A = \{v_1, v_2, \dots, v_n\}$ generates V then some subset of A is a basis for V.

Solution. For that, let declare the next set:

$$S = \{W \in \mathcal{P}(A) | W \text{ is linearly independent}\}$$

We can assure that at least there is a maximal element $\{v_1, v_2, \dots, v_m\}$ in S since we can assure the existence of $\{v_1\}$ and at most it can be A. Suppose then that it is not A, so $m < n$, and we can assure that any set $\{v_1, \dots, v_m, v_i\}$ is linearly dependent, with $m < i \leq n$. Therefore we have:

$$a_1v_1 + \cdots + a_nv_n + a_iv_i = 0$$

has more than the trivial solution, so we can suppose that

<u>Problem 4:</u> Let $A = \{v_1, v_2, \dots, v_n\}$ be a subset of a vector space V. Prove that A is linearly independent if and only if the equation $a_1v_1 + a_2v_2 + \cdots + a_nv_n = 0$ has the trivial solution.

Solution. We prove a double implication:

$\Rightarrow$) If A is linearly independent then by definition the equation $a_1v_1 + a_2v_2 + \cdots + a_nv_n = 0$ has only one solution, the trivial one.

$\Leftarrow$) Suppose that A is not linearly independent, so that there are two combinations of scalars $a_1, a_2, \dots, a_n$ and $b_1, b_2, \dots, b_n$ such that for a v in V:

$$\begin{aligned}
a_1v_1 + a_2v_2 + \cdots + a_nv_n &= v \\
b_1v_1 + b_2v_2 + \cdots + b_nv_n &= v
\end{aligned}$$

And if we use the transitivity we have:

$$\begin{aligned}
a_1v_1 + a_2v_2 + \cdots + a_nv_n &= b_1v_1 + b_2v_2 + \cdots + b_nv_n \\
(a_1 - b_1)v_1 + (a_2 - b_2)v_2 + \cdots + (a_n - b_n)v_n &= 0
\end{aligned}$$

But note that $a_1 \neq b_1$, $a_2 \neq b_2$ and so on, so $a_1 - b_1 \neq 0$, $a_2 - b_2 \neq 0$ and so on, so the equation has another solution apart to the trivial one.

Problem 5: Prove the Rank theorem

Solution. Remember that the rank theorem says that if V and W are finite dimensional vector spaces over K, and $\phi : V \to W$ is a linear map then:

$$\dim V = \dim \ker(\phi) + \dim \phi(V)$$

Let $\mathcal{A} = \{v_1, v_2, \dots, v_n\}$ be a basis for $ker(\phi)$ and let $\mathcal{B} = \{w_1, w_2, \dots, w_m\}$ be a basis for $\phi(V)$. Since $\mathcal{B} \subseteq \phi(V)$ there are $u_1, u_2, \dots, u_m$ such that $\phi(u_1) = w_1, \phi(u_2) = w_2, \dots, \phi(u_m) = w_m$. So, we can create the set:

$$\mathcal{C} = \{v_1, v_2, \dots, v_n, u_1, u_2, \dots, u_m\}$$

And we claim that this is a basis for V. For that, let's prove the two properties for that:

- Suppose that there are scalars $a_1, a_2, \dots, a_n, b_1, \dots, b_m$ such that:

$$\begin{aligned}
a_1v_1 + a_2v_2 + \cdots + a_nv_n + b_1u_1 + b_2u_2 + \cdots + b_mu_m = 0 \\
a_1v_1 + a_2v_2 + \cdots + a_nv_n &= -b_1u_1 - b_2u_2 - \cdots - b_mu_m \\
\phi(a_1v_1) + \phi(a_2v_2) + \cdots + \phi(a_nv_n) &= \phi(-b_1u_1) + \phi(-b_2u_2) + \cdots + \phi(-b_mu_m) \\
a_1\phi(v_1) + a_2\phi(v_2) + \cdots + a_n\phi(v_n) &= -b_1\phi(u_1) - b_2\phi(u_2) - \cdots - b_n\phi(u_m) \\
a_10 + a_20 + \cdots + a_n0 &= -b_1w_1 - b_2w_2 - \cdots - b_mw_m \\
0 &= -b_1w_1 - b_2w_2 - \cdots - b_mw_m
\end{aligned}$$

  And since $\mathcal{B}$ is a basis then $b_1 = b_2 = \cdots = b_m = 0$. And therefore we have that:

$$\begin{aligned}
a_1v_1 + a_2v_2 + \cdots + a_nv_n + b_1u_2 + b_2u_2 + \cdots + b_mu_m &= 0 \\
a_1v_1 + a_2v_2 + \cdots + a_nv_n &= 0
\end{aligned}$$

  And since $\mathcal{A}$ is a basis, then $a_1 = a_2 = \cdots = a_n = 0$, and so $\mathcal{C}$ is linearly independent.

- Take $v \in V$, we want to prove it is a linear combination of elements of $\mathcal{C}$. So for that, we know that $\phi(v)$ is a linear combination of elements of $\mathcal{B}$:

$$\begin{aligned}
b_1w_1 + b_2w_2 + \cdots + b_mw_m &= \phi(v) \\
b_1\phi(u_1) + b_2\phi(u_2) + \cdots + b_m\phi(u_m) &= \phi(v) \\
\phi(b_1u_1 + b_2u_2 + \cdots + b_mu_m) &= \phi(v) \\
\phi(b_1u_1 + b_2u_2 + \cdots + b_mu_m) - \phi(v) &= 0 \\
\phi(b_1u_1 + b_2u_2 + \cdots + b_mu_m - v) &= 0
\end{aligned}$$

  And since $b_1u_1 + b_2u_2 + \cdots + b_mu_m - v \in \ker(\phi)$ we can derive a linear combination of the form:

$$\begin{aligned}
a_1v_1 + a_2v_2 + \cdots + a_nv_n &= b_1u_1 + b_2u_2 + \cdots + b_mu_m - v \\
a_1v_1 + a_2v_2 + \cdots + a_nv_n - b_1u_1 - b_2u_2 - \cdots - b_mu_m &= -v \\
b_1u_1 + b_2u_2 + \cdots + b_mu_m - a_1v_1 - a_2v_2 - \cdots - a_nv_n &= v
\end{aligned}$$

  And so we have that v is a linear combination of $\mathcal{C}$, so $Span(\mathcal{C}) = V$.

And that way we conclude that $\mathcal{C}$ is a basis for V and note that $|\mathcal{C}| = |\mathcal{A}| + |\mathcal{B}|$, so $\dim V = \dim \ker(\phi) + \dim \phi(V)$.

Problem 6: Determine whether or not $\{(1, 1, 0), (2, 0, -1), (-3, 1, 1)\}$ is basis for $\mathbb{R}^3$

Solution. First, let's determine whenever it is linearly independent or not.

- Suppose that $a_1(1,1,0)+a_2(2,0,-1)+a_3(-3,1,1)=0$. So, if we add those vectors we would have:

$$\begin{aligned}a_1(1,1,0)+a_2(2,0,-1)+a_3(-3,1,1) &= (a_1,a_1,0)+(2a_2,0,-a_2)+(-3a_3,a_3,a_3)\\ &= (a_1+2a_2-3a_3, a_1+a_3, -a_2+a_3)=(0,0,0)\end{aligned}$$

  So we would need that:

$$\begin{aligned}a_1+2a_2-3a_3&=0\\ a_1+a_3&=0\\ a_3-a_2&=0\end{aligned}$$

  If we solve the last two equations for a_1 and a_2 we would have:

$$\begin{aligned}a_1&=-a_3\\ a_2&=a_3\end{aligned}$$

  And replacing in the first equation we would have:

$$\begin{aligned}a_1+2a_2-3a_3&=0\\ -a_3+2a_3-3a_3&=0\\ -2a_3&=0\\ a_3&=0\end{aligned}$$

  And so we conclude that $a_1=a_2=a_3=0$, so this set is linearly independent.

- Take now any vector $(x,y,z)\in\mathbb{R}^3$, we want to prove that we can always find a linear combination of the vectors that give us (x,y,z). For that, suppose that there are such combinations, so:

$$\begin{aligned}a_1(1,1,0)+a_2(2,0,-1)+a_3(-3,1,1)&=(x,y,z)\\ (a_1,a_1,0)+(2a_2,0,-a_2)+(-3a_3,a_3,a_3)&=(x,y,z)\\ (a_1+2a_2-3a_3,a_1+a_3,a_3-a_2)&=(x,y,z)\end{aligned}$$

  And so we have:

$$\begin{aligned}a_1+2a_2-3a_3&=x\\ a_1+a_3&=y\\ a_3-a_2&=z\end{aligned}$$

  Then we have:

$$\begin{aligned}a_1&=y-a_3\\ a_2&=a_3-z\end{aligned}$$

  And plugging into the first equation we have:

$$\begin{aligned}a_1+2a_2-3a_3&=x\\ y-a_3+2(a_3-z)-3a_3&=x\\ y-a_3+2a_3-2z-3a_3&=x\\ y-2z-2a_3&=x\\ a_3&=\frac{2z-x-y}{2}\end{aligned}$$

  And plugging into the next equation:

$$\begin{aligned}a_1&=y-a_3\\ a_1&=y-\frac{x+y-2z}{2}\\ a_1&=y+z-\frac{x}{2}+\frac{y}{2}\\ a_1&=\frac{3}{2}y+z-\frac{x}{2}\end{aligned}$$

And plugging into the last equation:

$$a_2 = a_3 - z$$
$$a_2 = z - \frac{x}{2} - \frac{y}{2} - z$$
$$a_2 = \frac{-x-y}{2}$$

And if you try this combination, you would get (x, y, z) so we can see $Span(\{(1,1,0),(2,0,-1),(-3,1,1)\}) = \mathbb{R}^3$.

And so we have proved that $\{(1,1,0),(2,0,-1),(-3,1,1)\}$ is a basis for $\mathbb{R}^3$.

<u>Problem 7:</u> Let $\phi : V \to W$ be linear. Suppose that $v_1, \ldots, v_n \in V$ are such that $\phi(v_1), \ldots, \phi(v_n)$ are linearly independent in W. Show that $v_1, \ldots, v_n$ are linearly independent.

Solution. For that, since $\phi(v_1), \ldots, \phi(v_n)$ are linearly independent, we can assure that the equation:

$$a_1\phi(v_1) + a_2\phi(v_2) + \cdots + a_n\phi(v_n) = 0$$

has only the trivial solution. Suppose that the equation:

$$b_1v_1 + b_2v_2 + \cdots + b_nv_n = 0$$

has a solution that is not trivial. That this, we can assure that at least b_1 is not 0. And if we apply to both sides the linear map ϕ we get:

$$\phi(b_1v_1 + b_2v_2 + \cdots + b_nv_n) = \phi(0)$$
$$\phi(b_1v_1) + \phi(b_2v_2) + \cdots + \phi(b_nv_n) = 0$$
$$b_1\phi(v_1) + b_2\phi(v_2) + \cdots + b_n\phi(v_n) = 0$$

But this is a contradiction since this equation can only have the trivial solution. So we can conclude that $v_1, \ldots v_n$.

<u>Problem 8:</u> If $\{v_1, \ldots, v_n\}$ is a basis for V and $\{w_1, \ldots, w_m\}$ is a basis for W then:

$$\{(v_1, 0), \ldots, (v_n, 0), (0, w_1), \ldots, (0, w_n)\}$$

is a basis for $V \oplus W$

Solution. We need to prove two things:

- First, to prove that this set is linearly independent, we need to show that the homogeneous equation has only the trivial solution. So we have:

$$a_1(v_1,0) + a_2(v_2,0) + \cdots + a_n(v_n,0) + b_1(0,w_1) + b_2(0,w_2) + \cdots + b_n(0,w_n) = (0,0)$$
$$(a_1v_1,0) + (a_2v_2,0) + \cdots + (a_nv_n,0) + (0,b_1w_1) + (0,b_2w_2) + \cdots + (0,b_nw_n) = (0,0)$$
$$(a_1v_1 + a_2v_2 + \cdots + a_nv_n, b_1w_1 + b_2w_2 + \cdots + b_nw_n) = (0,0)$$

  And this means that:

$$a_1v_1 + a_2v_2 + \cdots + a_nv_n = 0$$
$$b_1w_1 + b_2w_2 + \cdots + b_nw_n = 0$$

  And since those vectors are basis for each vector space $a_1 = a_2 = \cdots = a_n = b_1 = b_2 = \cdots = b_n$.

- For an element $(v, w) \in V \oplus W$, we know that v can be expressed as a linear combination $a_1v_1 + a_2v_2 + \cdots + a_nv_n = v$, and also w can be expressed as $b_1w_1 + b_2w_2 + \cdots + b_nv_n = w$, so the combination of the vectors in our set will rise:

$$a_1(v_1,0) + a_2(v_2,0) + \cdots + a_n(v_n,0) + b_1(0,w_1) + b_2(0,w_2) + \cdots + b_n(0,w_n) = (v,w)$$

Problem 9: Let W be a subspace of the finite-dimensional vector space V. Show that there is a subspace U of V such that $V \cong U \oplus W$.

Solution. For this, define U as follows:

$$U := V \setminus W \cup \{0\}$$

First, we need to prove that this is a subspace of V:

> Note that for any $v \in U$ different from 0 and any $c \in K$, if $cv \in W$ then $c^{-1}cv = v \in W$ which contradicts the definition of U. If $u, w \in U$ are not both 0, and if $u + w \in W$ then that means that $u, w \in W$ since W is closed over the operations, which again, contradicts the definition for U, so $u + w \in U$.

Now, we want to prove that this is an internal sum of V, so we have:

- If $w \in W$ and $u \in U$ are such that $w + u = 0$, then we would have $w = -u$, which means that $w \in U$ and also that $u = -w \in V$, which means that since its only common element is 0, $u = w = 0$.
- For any element $v \in V$, there are two alternatives. If $v \in W$ then we can express v as $v + 0$ and $0 \in U$. If $v \notin W$ then $v \in U$ by definition and so $v = 0 + v$ with $0 \in W$.

And so we conclude that $U \oplus W$ is an internal sum of V.

Problem 10: A linear map $\rho : V \to V$ is idempotent if $\rho\rho = \rho$. Show that ρ acts as an identity over $\rho(V)$ if ρ is idempotent.

Solution. For that, we want to prove that $\rho^2 = Id_{\rho(V)}$. For that, let $v \in \rho(V)$, we know that there is $w \in V$ such that $\rho(w) = v$. Now, if we apply again the function we would have:

$$\begin{aligned} \rho(\rho(w)) &= \rho(v) \\ \rho(w) &= \rho(v) \\ v &= \rho(v) \end{aligned}$$

So we conclude that $\rho^2 = Id_{\rho(V)}$.

Problem 11: Decide if $\phi : \mathbb{R}^2 \to \mathbb{R}^2$ given by $\phi(x, y) = (x + y, 2x - y)$ is an isomorphism. If it is, find a formula for $\phi^{-1}(x, y)$ and prove they are inverses.

Solution. Suppose that for a vector $(a, b) \in \mathbb{R}^2$, exists $(x, y) \in \mathbb{R}^2$ whose image under ϕ is (a, b). We would have:

$$\phi(x, y) = (x + y, 2x - y) = (a, b)$$

And so we can write the next equations:

$$\begin{aligned} x + y &= a \\ 2x - y &= b \end{aligned}$$

If we solve for x in the first equation we would have:

$$x = a - y$$

And replacing in the second equation we would have:

$$\begin{aligned} 2x - y = 2(a - y) - y &= b \\ 2a - 2y - y &= b \\ 2a - 3y &= b \\ -3y &= b - 2a \\ y &= \frac{2a - b}{3} \end{aligned}$$

And so if we plug in into the second equation we would have:

$$\begin{aligned} x &= a - y \\ &= a - \frac{2a-b}{3} \\ &= a - \frac{2a}{3} + \frac{b}{3} \\ &= \frac{a}{3} + \frac{b}{3} \\ &= \frac{a+b}{3} \end{aligned}$$

And so we would have:

$$\phi^{-1}(x,y) = \left(\frac{x+y}{3}, \frac{2x-y}{3} \right)$$

We can prove also that this indeed the inverse isomorphism by composing them:

- First, if we compose ϕ and ϕ^{-1} we would have:

$$\begin{aligned} \phi(\phi^{-1}(x,y)) &= \phi\left(\frac{x+y}{3}, \frac{2x-y}{3} \right) \\ &= \left(\frac{x+y}{3} + \frac{2x-y}{3}, 2 \cdot \frac{x+y}{3} - \frac{2x-y}{3} \right) \\ &= \left(\frac{3x}{3}, \frac{2x+2y}{3} + \frac{y-2x}{3} \right) \\ &= \left(x, \frac{3y}{3} \right) \\ &= (x,y) \end{aligned}$$

- And now, if we compose ϕ^{-1} and ϕ we get:

$$\begin{aligned} \phi^{-1}(\phi(x,y)) &= \phi^{-1}(x+y, 2x-y) \\ &= \left(\frac{x+y+2x-y}{3}, \frac{2(x+y)-(2x-y)}{3} \right) \\ &= \left(\frac{3x}{3}, \frac{2x+2y-2x+y}{3} \right) \\ &= \left(x, \frac{3y}{3} \right) \\ &= (x,y) \end{aligned}$$

So we conclude that ϕ and ϕ^{-1} are inverses and so they are isomorphisms.

Problem 12: Let V be a vector space over a field k and let U, W be finite dimensional subspaces of V. Prove that both $U+W$ and $U \cap W$ are finite-dimensional subspaces of V and that

$$\dim(U+W) + \dim(U \cap W) = \dim U + \dim W$$

Solution. First, note that if $U \cap W$ is the empty set, then its dimension is 0 and so it is finite-dimensional. Suppose it is not empty, so there is at least one $v \in U \cap W$. If we suppose that $\mathcal{B}$ is an infinite basis for $U \cap W$ then v is a linear combination of the elements in $\mathcal{B}$. But also $v \in U$ but this would be a contradiction because this implies that $\mathcal{B}$ is linearly dependent and so it cannot be a basis for $U \cap W$.

Now, we can find basis for each vector spaces as follows:

$$\begin{aligned}\mathcal{B} &= \{v_1, \dots, v_k\}(\text{Basis for } U \cap W)\\ \mathcal{B}_1 &= \{v_1, \dots, v_k, u_1, \dots, u_n\}(\text{Basis for } U\text{, since we can extend any basis})\\ \mathcal{B}_2 &= \{v_1, \dots, v_k, w_1, \dots, w_m\}(\text{Basis for } W\text{, since we can extend any basis})\end{aligned}$$

We are going to prove that $\mathcal{A} = \{v_1, \dots, v_k, u_1, \dots, u_n, w_1, \dots, w_m\}$ is a basis for $U + W$.

- First, suppose that $a_1, \dots, a_k, b_1, \dots b_n, c_1, \dots, c_m$ are scalars in k such that:

$$a_1v_1 + \dots + a_kv_k + b_1u_1 + \dots + b_nu_n + c_1w_1 + \dots + c_mw_m = 0$$

  Suppose with no lose of generality that $a_1 \neq 0$, so we can express v_1 in the next way:

$$v_1 = \frac{-a_2v_2 - \dots - a_kv_k - b_1u_1 - \dots - b_nu_n - c_1w_1 - \dots - c_mw_m}{a_1}$$

  But note that $v_1 \in U$ and $v_1 \in W$, so we can assure that

- For any element $v \in U + W$, we can express it as $u + w$ with $u \in U$ and $w \in W$. Now, for that we can express u and w as:

$$\begin{aligned}u &= a_1v_1 + a_2v_2 + \dots + a_kv_k + x_1u_1 + x_2u_2 + \dots + x_nu_n\\ w &= b_1v_1 + b_2v_2 + \dots + b_kv_k + y_1w_1 + y_2w_2 + \dots + y_mw_m\end{aligned}$$

  And if we add them up we get:

$$\begin{aligned}u + w &= a_1v_1 + a_2v_2 + \dots + a_kv_k + x_1u_1 + x_2u_2 + \dots + x_nu_n + b_1v_1 + b_2v_2 + \dots + b_kv_k + y_1w_1 + y_2w_2 + \dots + y_mw_m\\ v &= (a_1 + b_1)v_1 + (a_2 + b_2)v_2 + \dots + (a_k + b_k)v_k + x_1u_1 + x_2u_2 + \dots + x_nu_n + y_1w_1 + y_2w_2 + \dots + y_mw_m\end{aligned}$$

  And so we have proved that $Span(\mathcal{A}) = U + W$.

Therefore, we conclude that $\mathcal{A}$ is a basis for $U + W$. But since the basis for U and the basis for W includes both the basis for $U \cap W$, we need to extract it, so:

$$\begin{aligned}\dim(U + W) &= \dim U + \dim W - \dim(U \cap W)\\ \dim(U + W) + \dim(U \cap W) &= \dim U + \dim W\end{aligned}$$

Problem 13: Let $\phi \in End(V)$ for a finite dimensional vector space V. Prove that ϕ is monic if and only if it is epic if and only if it is an isomorphism

Solution. Since V is a finite dimensional vector space we can use the rank theorem to find the dimensions of the kernel, images and V.

- Suppose that ϕ is monic, so that $\ker(\phi) = \{0\}$. We would have then that $\dim \ker(\phi) = 0$ and so $\dim V = \dim \phi(V)$, and since $\phi(V) \subseteq V$ we conclude that $\phi(V) = V$ so that ϕ is epic.
- Suppose that ϕ is epic, so that $\phi(V) = V$. We would have then that $\dim \ker(\phi) = 0$, and since $\ker(\phi)$ is a subspace of V, if there would be a vector different from 0 into the set, it would make a basis and so $\dim \ker(\phi) > 0$, so we would only have that $\ker(\phi) = \{0\}$ and so ϕ is monic.
- If we suppose that ϕ is monic or epic, we get the other one and so it is an isomorphism. If it is an isomorphism we are granted that it is monic and epic.

Problem 14: If $\phi : \mathbb{R}^2 \to \mathbb{R}^2$ is defined as $\phi(x, y) = (x + y, 2x - y)$ then determine what is $p(\phi)$ when $p(x) = x^2 - 2x + 1$

Solution. Note that $\phi^2 = \phi \circ \phi$ and so $\phi^0 = Id_{\mathbb{R}^2}$, and we can write the polynomial as:

$$p(x) = x^2 - 2x + 1x^0$$

So if we apply it to ϕ we would have:

$$\begin{aligned} p(\phi(x, y)) &= \phi^2(x, y) - 2\phi(x, y) + 1\phi^0(x, y) \\ &= \phi(x + y, 2x - y) - 2(x + y, 2x - y) + 1(x, y) \\ &= (3x, 3y) + (-2x - 2y, 2y - 4x) + (x, y) \\ &= (3x - 2x - 2y + x, 3y + 2y - 4x + y) \\ &= (2x - 2y, 6y - 4x) \end{aligned}$$

Problem 15: Show that the set $V(\lambda)$ is a subspace of V for each $\lambda \in K$.

Solution. Suppose that for a fixed $\lambda \in K$ and an endomorphism $\phi : V \to V$, $v, w \in V(\lambda)$. Then $\phi(v) = \lambda v$ and $\phi(w) = \lambda w$. Suppose also that $k \in K$, so we want to show that $cv + w \in V(\lambda)$. So, we need to prove that this vector under ϕ is the same vector scaled in λ:

$$\begin{aligned} \phi(cv + w) &= c\phi(v) + \phi(w) \\ &= c\lambda v + \lambda w \\ &= \lambda(cv + w) \end{aligned}$$

And so we get that $\phi(cv + w) = \lambda(cv + w)$ and so $V(\lambda)$ is a subspace of V.

Problem 16: Given $\phi \in End(V)$, show that 0 is an eigenvalue for ϕ if and only if $\ker \phi \neq \{0\}$.

Solution. Suppose that $\ker \phi \neq \{0\}$, then there is some $v \in V$ such that $v \neq 0$ and $\phi(v) = 0$. Then, $\phi(v) = 0v$ and so v is an eigenvector with eigenvalue 0. Now, if 0 is an eigenvalue for ϕ then there is $v \in V$ no null such that $\phi(v) = 0v$ but this is $\phi(v) = 0$ and so $\ker \phi \neq \{0\}$.

Problem 17: Suppose that λ is an eigenvalue for an isomorphism $\phi \in GL(V)$. Show that λ^{-1} is an eigenvalue for ϕ^{-1}.

Solution. If λ is an eigenvalue for ϕ, then there is a no null vector v such that $\phi(v) = \lambda v$. Now, if we compute:

$$\begin{aligned} \phi^{-1}(\phi(v)) &= v \\ &= (\lambda^{-1}\lambda)v \\ &= \lambda^{-1}(\lambda v) \\ &= \lambda^{-1}\phi(v) \end{aligned}$$

So we conclude that λ^{-1} is an eigenvalue for ϕ^{-1} with eigenvector $\phi(v)$.

Problem 18: Let $\{e_1, e_2, e_3\}$ be the standard basis for $\mathbb{R}^3$. Find the eigenvalues with their correspondent eigenvectors for $\phi : \mathbb{R}^3 \to \mathbb{R}^3$ defined by $\phi(e_1) = e_1$, $\phi(e_2) = e_1 + e_2$ and $\phi(e_3) = e_3$. What is the geometric multiplicity of each eigenvalue?

Solution. So, we first need to characterize the transformation for any vector in $\mathbb{R}^3$. Let $\alpha = (a_1, a_2, a_3)$

be a vector in $\mathbb{R}^3$ then:

$$\begin{aligned}\phi(\alpha) &= \phi(a_1e_1 + a_2e_2 + a_3e_3)\\ &= a_1\phi(e_1) + a_2\phi(e_2) + a_3\phi(e_3)\\ &= a_1e_1 + a_2(e_1+e_2) + a_3e_3\\ &= (a_1+a_2)e_1 + a_2e_2 + a_3e_3\end{aligned}$$

And we want to see whenever it is equal to the same vector scaled by α:

$$\begin{aligned}(a_1+a_2)e_1 + a_2e_2 + a_3e_3 &= \lambda(a_1e_1 + a_2e_2 + a_3e_3)\\ (a_1+a_2)e_1 + a_2e_2 + a_3e_3 &= \lambda a_1e_1 + \lambda a_2e_2 + \lambda a_3e_3\end{aligned}$$

From which we get:

$$\begin{aligned}a_1 + a_2 &= \lambda a_1\\ a_2 &= \lambda a_2\\ a_3 &= \lambda a_3\end{aligned}$$

And so we get:

$$\begin{aligned}a_1(1-\lambda) + a_2 &= 0\\ a_2(1-\lambda) &= 0\\ a_3(1-\lambda) &= 0\end{aligned}$$

In any case no matter the values for α, we get that $\lambda = 1$, and the eigenvectors associated with λ are e_1 and e_3. Therefore, the geometric multiplicity of $V(1)$ is 2.

1 Groups, Rings and Polynomials

Problem 19: If $(G, \circledcirc)$ and $(H, \circledast)$ are groups, and $\phi : G \to H$ a group homomorphism, prove that $\Im(\phi)$ is a subgroup of H. Is it normal?

Solution. Suppose that $h_1, h_2 \in Im(\phi)$, then there are $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. Now, we want to prove that $h_1 \circledast h_2 \in Im(\phi)$, so if we compute:

$$\begin{aligned}\phi(g_1 \circledcirc g_2) &= \phi(g_1) \circledast \phi(g_2)\\ &= h_1 \circledast h_2\end{aligned}$$

So we conclude that $Im(\phi)$ is closed under $\circledast$. If we have $h \in Im(\phi)$ then there is $g \in G$ such that $\phi(g)$. If we compute the image for the inverse of g as follows, we get:

$$\begin{aligned}e_H &= h \circledast h^{-1}\\ \phi(e_G) &= \phi(g) \circledast h^{-1}\\ \phi(g^{-1}) \circledast \phi(e_G) &= \phi(g^{-1}) \circledast \phi(g) \circledast h^{-1}\\ \phi(g^{-1} \circledcirc e_G) &= \phi(g^{-1} \circledcirc g) \circledast h^{-1}\\ \phi(g^{-1}) &= \phi(e_G) \circledast h^{-1}\\ \phi(g^{-1}) &= e_H \circledast h^{-1}\\ \phi(g^{-1}) &= h^{-1}\end{aligned}$$

And so we conclude that the $h^{-1} \in Im(\phi)$ so $Im(\phi)$ is a subgroup of H. If H is commutative then $Im(\phi)$ is a normal group.

<u>Problem 20:</u> Let G be a group and X a nonempty set. Then G acts from the left on X if there is a function

$$G \times X \to X, (g, x) \mapsto g \cdot x$$

such that the following hold:

- $e \cdot x = x$ for all $x \in X$
- $g \cdot (h \cdot x) = (gh) \cdot x$ for all $g, h \in G$ and $x \in X$

Show that $x \mapsto g \cdot x$ is a bijection on X with inverse $x \mapsto g^{-1} \cdot x$. Also, for $x \in X$, $G \cdot x$ is called the orbit of x under the action of G. Show that the relation y *is in the orbit of* x is an equivalence relation X.

Solution. First, we are going to prove that this is a bijection.

- Suppose that $x, y \in X$ are elements that have the same image. Then $g \cdot x = g \cdot y$ if we multiply by the inverse element of g under G we get that $x = y$.
- Take $x \in X$, then since $g^{-1} \cdot x \in X$, we can apply the function to it and we get $g \cdot (g^{-1} \cdot x) = (g \cdot g^{-1}) \cdot x = e \cdot x = x$.

So that function is a bijection. If we compose it to the right and to the left with the other one it is obvious that we get the identity map over X so they are inverses.

And now we are going to prove that it is an equivalence relation:

- **Reflexivity:** Since $e \cdot x = x$ then $x \in G \cdot x$
- **Symmetry:** Suppose $y \in G \cdot x$, then there is $g \in G$ such that $g \cdot x = y$. If we manipulate it as follows:

$$\begin{aligned} g \cdot x &= y \\ g^{-1} \cdot (g \cdot x) &= g^{-1} \cdot y \\ (g^{-1} \cdot g) \cdot &= g^{-1} \cdot y \\ e \cdot x &= g^{-1} \cdot y \\ x &= g^{-1} \cdot y \end{aligned}$$

  And since $g^{-1} \in G$ then $x \in G \cdot y$.

- **Transitivity:** Suppose that $y \in G \cdot x$ and $z \in G \cdot y$, so there are $g_1, g_2 \in G$ such that $y = g_1 \cdot x$ and $z = g_2 \cdot y$. And so if we replace the value of y then:

$$\begin{aligned} z &= g_2 \cdot y \\ &= g_2 \cdot (g_1 \cdot x) \\ &= (g_2 \cdot g_1) \cdot x \end{aligned}$$

  And so $z \in G \cdot x$.

<u>Problem 21:</u> Show that if H is a subgroup of G, then $(h, g) \mapsto h \cdot g$ and $(h, g) \mapsto hgh^{-1}$ define actions of H on G.

Solution. For the first function:

- Since H is a subgroup of G, then $e \in H$ is also the identity of G and so $(e, g) \mapsto e \cdot g = g$.
- Thanks to the fact that H is a subgroup of G, $(h_2, (h_1, g)) \mapsto h_2 \cdot (h_1, g) = h_2 \cdot (h_1 \cdot g) = (h_2 \cdot h_1) \cdot g$.

And so the first function define an action over G. And for the second function:

- Since H is a subgroup of G, $(e, g) \mapsto e \cdot x \cdot e^{-1} = e \cdot x \cdot e = x$.
- Thanks to the fact that H is a subgroup of G, $(h_2, (h_1, g)) \mapsto h_2(h_1, g)h_2^{-1} = h_2(h_1 \cdot g \cdot h_1^{-1})h_2^{-1}$ and by properties of the group that is equal $(h_2h_1) \cdot g \cdot (h_1^{-1}h_2^{-1}) = (h_2h_1) \cdot g \cdot (h_2h_1)^{-1}$.

<u>Problem 22:</u> Show that:

$$\mathfrak{S}_m \times \mathbb{N}^m \to \mathbb{N}^m \qquad (\sigma, \alpha) \mapsto \sigma \cdot \alpha := (\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(m)})$$

defines an action of $\mathfrak{S}_m$ on $\mathbb{N}^m$.

Solution. Proving the two properties:

- $Id_m \cdot \alpha = (\alpha_{Id_m(1)}, \ldots, \alpha_{Id_m(m)}) = (\alpha_1, \ldots, \alpha_m)$ and so we conclude that $Id_m \cdot \alpha = \alpha$
- For prove the associativity of the operation we get:

$$\begin{aligned}
\sigma \cdot (\pi \cdot \alpha) &= \sigma \cdot (\alpha_{\pi(1)}, \ldots, \alpha_{\pi(m)}) \\
&= (\alpha_{\pi(\sigma(1))}, \ldots, \alpha_{\pi(\sigma(m))}) \\
&= (\pi \cdot \sigma) \cdot \alpha
\end{aligned}$$

So $\mathfrak{S}_m$ acts over $\mathbb{N}^m$.

<u>Problem 23:</u> Let G and H be groups, and let:

$$p : G \times H \to G, \qquad (g, h) \mapsto g$$

be the projection onto the first factor. Show that p is a surjective homomorphism. Set $H' := \ker(p)$. Show that $(G \times H)/H'$ and G are isomorphic group.

Solution. First, for any $g \in G$, the ordered pair (g, e_H) will project to g so p is surjective. We are going to prove that it is also an homomorphism:

$$\begin{aligned}
p(g_1 \circledcirc g_2, h_1 \circledast h_2) &= g_1 \circledcirc g_2 \\
&= p(g_1, h_1) \circledcirc p(g_2, h_2)
\end{aligned}$$

Now, note that the kernel $ker(p) = \{(g, h) \in G \times H | g = 0_G\}$ and so if we seek the relation over the kernel of the map we see that if $(x_1, x_2) \sim (y_1, y_2)$ then:

$$\begin{aligned}
(x_1, x_2) \in (y_1, y_2) \circleddash H' \Leftrightarrow (x_1, x_2) &= (y_1, y_2) \circleddash (0, h) \\
(x_1, x_2) &= (y_1, y_2 \circledast h)
\end{aligned}$$

and so we get that $x_1 = y_1$ and $x_2 = y_2 \circledast h$, so we can conclude that are elements that have the same image, that is $[(x, y)] = \{(g, h) \in G \times H | g = x\}$.

$$\phi : (G \times H)/H' \to G \qquad [(x, y)] \mapsto x$$

So, we need to prove that it is a bijective homomorphism:

- **Injectivity:** Suppose that $[(x,y)]$ and $[(z,w)]$ elements from $(G \times H)/H'$ have the same image. So it means that $x = z$ and therefore $[(x,y)] = [(z,w)]$.
- **Surjective:** For any $g \in G$, you get that $\phi([(g, e_H)]) = g$ so ϕ is surjective
- **Homomorphism:** For $[(x,y)]$ and $[(z,w)]$ elements from $(G \times H)/H'$ compute the image of its product:

$$\begin{aligned}\phi([(x,y)] \ominus [(z,w)]) &= \phi([(x \circledcirc z, y \circledast z)]) \\ &= x \circledcirc z \\ &= \phi([(x,y)]) \circledcirc \phi([(z,w)])\end{aligned}$$

So we conclude that $(G \times H)/H'$ and G are isomorphic.

Problem 24: Let G be a set with an operation $\circledcirc$ and identity element. For $g \in G$, define the function $Lg : G \to G$, $h \mapsto g \circledcirc h$ called the **left transition** by g. Define then the set:

$$L := \{Lg \in Func(G,G) | g \in G\}$$

Prove that $(G, \circledcirc)$ is a group if and only if $L \subseteq \mathfrak{S}_G$.

Solution.

$\Rightarrow$) If $(G, \circledcirc)$ is a group, then we need to prove that for any g, Lg is a bijection. First, the injectivity since if $Lg(h) = Lg(k)$ then $g \circledcirc h = g \circledcirc k$ and therefore $h = k$. Now, for any element h in the group, $Lg(g^{-1} \circledcirc h) = g \circledcirc (g^{-1} \circledcirc h) = (g \circledcirc g^{-1}) \circledcirc h = e \circledcirc h = h$, and so Lg is a bijection and therefore $L \subseteq \mathfrak{S}_G$.

$\Leftarrow$) If $L \subseteq \mathfrak{S}_G$ then for any $g \in G$, the function Lg is bijective and so it has an inverse, call it Rg. That function is also a bijection and so it is surjective. So, for any g, the there is $g \circledcirc h \in G$ such that $Rg(g \circledcirc h) = e$. But this means that $Lg(h) = g \circledcirc h = e$ and so we conclude that each element has an inverse element.

2 Rings and Fields

Problem 25: Let a, b be commuting elements of a ring with unity and $n \in \mathbb{N}$, prove that:

1. $a^{n+1} - b^{n+1} = (a-b)\sum_{j=0}^{n} a^j b^{n-j}$
2. $a^{n+1} - 1 = (a-1)\sum_{j=0}^{n} a^j$

Solution. We prove the first one by induction. If $n = 0$, then we would have:

$$\begin{aligned}(a-b)\sum_{j=0}^{0} a^j b^{n-j} &= (a-b)[a^0 b^0] \\ &= (a-b)\end{aligned}$$

which shows that the claim is true. Suppose it is true for n, and so we have:

$$\begin{aligned}
(a-b)\sum_{j=0}^{n+1} a^j b^{n+1-j} &= (a-b)\left[\sum_{j=0}^{n} a^j b^{n+1-j} + a^{n+1}\right] \\
&= (a-b)\sum_{j=0}^{n} a^j b^{n+1-j} + (a-b)a^{n+1} \\
&= b(a-b)\sum_{j=0}^{n} a^j b^{n-j} + (a-b)a^{n+1} \\
&= b(a^{n+1}-b^{n+1}) + a^{n+2} - a^{n+1}b \\
&= a^{n+1}b - b^{n+2} + a^{n+2} - a^{n+1}b \\
&= a^{n+2} - b^{n+2}
\end{aligned}$$

So the claim is true for all $n \in \mathbb{N}$. The second identity is a special case of the first one when $b = 1$.

Problem 26: For a ring R with unity, show that $(1-X)\sum_k X^k = (\sum_k X^k)(1-X) = 1$ in $R\|X\|$

Solution. For that, let's define:

$$q_n = (1-X) := \begin{cases} 1 & n = 0 \\ -1 & n = 1 \\ 0 & n \geq 2 \end{cases}$$

And also notice that:

$$p := \sum_k X^k = (1_R)_{n\in\mathbb{N}}$$

So if we compute the product pq we have:

- For $n = 0$ that is $(pq)_n = p_0 q_0 = 1$
- For $n = 1$ that is $(pq)_n = p_0 q_1 + p_1 q_0 = 1 \cdot 1 - 1 \cdot 1 = 0$
- For $n \geq 2$ that is $(pq)_n = p_0 q_n + p_1 q_{n-1} + \cdots + p_k q_{n-k} + \cdots + p_n q_0 = 1 - 1 + \cdots + 0 + \cdots + 0 = 0$

So we characterize this polynomial as:

$$(pq)_n := \begin{cases} 1 & n = 0 \\ 0 & n \geq 1 \end{cases}$$

Which means that $pq = X^0 = 1$. The same argument is applied to show that this result commutes.

Problem 27: Show that a finite field cannot be ordered.

Solution. Suppose that $(K, \leq)$ is a finite ordered field. Now, define the function $f : \mathbb{N} \to K^+$ recursively as:

$$\begin{aligned} f(0) &= 0 \\ f(n^+) &= f(n) + 1 \end{aligned}$$

Now, we can prove that this function is bijective. If $n, m \in \mathbb{N}$ are such that $f(n) = f(m)$ then:

- If $f(n) = f(m) = 0$ then we are done since $f(n^+) > 0$ for all $n \in \mathbb{N}$ so $n = m = 0$.

- Suppose that in general if $f(n) = f(m)$ then $n = m$. Now, if $f(n^+) = f(m)$ we must express m as x^+ for $x \in \mathbb{N}$ and so:

$$\begin{aligned} f(n^+) &= f(x^+) \\ f(n) + 1 &= f(x) + 1 \\ f(n) &= f(x) \end{aligned}$$

  And so by induction hypothesis, $n = x$ and so $n^+ = x^+ = m$ and therefore this statement is true in general.

But then we would have $\mathbb{N} \preccurlyeq K^+ \preccurlyeq K$ and so we would have that K is infinite which is a contradiction. Therefore, no finite field can be ordered.

<u>Problem 28:</u> Show that a polynomial ring in one indeterminate over a field has no zero divisors.

Solution. Suppose that p, q are polynomial over $K[X]$ with degree n and m respectively. Now, if we suppose that both Polynomials are distinct from 0, then we have:

$$\begin{aligned} (pq)_{n+m} &= \sum_{k=0}^{n+m} p_k q_{j-k} \\ &= p_0 q_{n+m} + p_1 q_{n+m-1} + \cdots + p_n q_m + \cdots + p_{n+m} q_0 \end{aligned}$$

Now, since K has no zero divisors, $p_n q_m \neq 0$ and for the terms we do the next analysis:

> The possible nonzero terms of p are $p_0, p_1, \ldots, p_n$ and all that is greater in its subindex is 0. Now, the possible nonzero terms of q are $q_0, q_1, \ldots, q_m$ and all that is greater in its subindex is 0. If $k < n$ then p_k is possibly nonzero, but $m < n + m - k$ so $q_{n+m-k} = 0$ and that term is just 0. And now if $k < m$ then q_m is defined but then $n < n + m - k$ and therefore p_{n+m-k} is 0. We conclude that the only nonzero term is $p_n q_m$.

And so since $(pq)_{m+n} \neq 0$ then $pq \neq 0$ and also this shows how $\deg(pq) = \deg(p) + \deg(q)$.

<u>Problem 29:</u> Let K be an ordered field and $a, b, c, d \in K$.

1. Show that, if $b > 0$ and $d > 0$ and $\frac{a}{b} < \frac{b}{d}$ then $\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}$
2. Show that if $a, b \in K^\times$ then $\left|\frac{a}{b} + \frac{b}{a}\right| \geq 2$

Solution.

1. For one side, since $\frac{a}{b} < \frac{c}{d}$ we have:

$$\begin{aligned} ad &< bc \\ ad + ab &< ab + bc \\ a(b + d) &< b(a + c) \end{aligned}$$

   And since $b > 0$ and $b + d > 0$ then we have:

$$\frac{a}{b} < \frac{a + c}{b + d}$$

   In a similar way one proves the other inequality.

2. Notice that we can decompose the left side as:

$$\begin{aligned}\left|\frac{a}{b}+\frac{b}{a}\right| &= \left|\frac{a^2+b^2}{ab}\right| \\ &= \frac{a^2+b^2}{|ab|} \\ &= \frac{a^2}{|ab|}+\frac{b^2}{|ab|}\end{aligned}$$

We will have three possible cases.

- If $\frac{a^2}{|ab|} \geq 1$ and $\frac{b^2}{|ab|} \geq 1$ then it is obviously true.
- If $\frac{a^2}{|ab|} \geq 1$ and $1 \geq \frac{b^2}{|ab|} \geq 0$ then $1-\frac{b^2}{|ab|} \leq 0$ and $\frac{a^2}{|ab|}-1 \geq 0$, so we conclude that $\frac{a^2}{|ab|}-1 \geq 1-\frac{b^2}{|ab|}$ and therefore $\frac{a^2}{|ab|}+\frac{b^2}{|ab|} \geq 2$.
- If $1 \geq \frac{a^2}{|ab|} \geq 0$ and $1 \geq \frac{b^2}{|ab|} \geq 0$ then we would have that:

$$\frac{1}{\frac{a^2}{|ab|}} \geq 1 \qquad\qquad \frac{1}{\frac{b^2}{|ab|}} \geq 0$$

$$\frac{|ab|}{a^2} \geq 1 \qquad\qquad \frac{|ab|}{b^2} \geq 1$$

And so we get that:

$$\begin{aligned}|ab|\left(\frac{1}{a^2}+\frac{1}{b^2}\right) &= |ab|\left(\frac{b^2+a^2}{a^2b^2}\right) \\ &= \frac{a^2}{|ab|}+\frac{b^2}{|ab|} \geq 2\end{aligned}$$

Problem 30: Let R be an ordered ring and $a, b \in R$ such that $a \geq 0$ and $b \geq 0$. Suppose that there is $n \in \mathbb{N}^\times$ such that $a^n = b^n$. Show that $a = b$.

Solution. The claim is obviously true when $a = 0$ or $b = 0$. Suppose that $a \neq 0$, $b \neq 0$ and $a^n = b^n$ for $n \in \mathbb{N}^\times$. That is:

$$\begin{aligned}a^n &= b^n \\ \frac{a^n}{b^n} &= 1 \\ \left(\frac{a}{b}\right)^n &= 1\end{aligned}$$

If n is odd then the only solution to this equation is 1, so that $\frac{a}{b} = 1$ and therefore $a = b$. But if n is even then -1 and 1 are solutions of the equation. But if $\frac{a}{b} = -1$ it means that $a = -b$ but this is a contradiction with the fact that $a \geq 0$ and $b \geq 0$, so it is only possible that $\frac{a}{b} = 1$ and therefore $a = b$.

Problem 31: Find $r, s \in K[X]$ with $\deg(r) < 3$ such that:

$$X^5 - 3X^4 + 4X^3 = s(X^3 - X^2 + X - 1) + r$$

Solution. We find them by construction. Set $s_1 = X^2$ and then set p_1 as:

$$\begin{aligned}p_1 &= p - qs_1 \\ &= (X^5 - 3X^4 + 4X^3) - X^2(X^3 - X^2 + X - 1) \\ &= X^5 - 3X^4 + 4X^3 - X^5 + X^4 - X^3 + X^2 \\ &= -2X^4 + 3X^3 + X^2\end{aligned}$$

Now, set $s_2 = -2X$ and set p_2 as follows:

$$\begin{aligned} p_2 &= p_1 - qs_2 \\ &= (-2X^4 + 3X^3 + X^2) + 2X(X^3 - X^2 + X - 1) \\ &= -2X^4 + 3X^3 + X^2 + 2X^4 - 2X^3 + 2X^2 - 2X \\ &= X^3 + 3X^2 - 2X \end{aligned}$$

And at last, set $s_3 = 1$ and set p_3 like:

$$\begin{aligned} p_3 &= p_2 - qs_3 \\ &= (X^3 + 3X^2 - 2X) - 1(X^3 - X^2 + X - 1) \\ &= X^3 + 3X^2 - 2X - X^3 + X^2 - X + 1 \\ &= 4X^2 - 3X + 1 \end{aligned}$$

Now, define $s := s_1 + s_2 + s_3$ and set $r := p_3$ then:

$$\begin{aligned} s(X^3 - X^2 + X - 1) + r &= (s_1 + s_2 + s_3)(X^3 - X^2 + X - 1) + r \\ &= (X^2 - 2X + 1)(X^3 - X^2 + X - 1) + 4X^2 - 3X + 1 \\ &= (X^5 - X^4 + X^3 - X^2 - 2X^4 + 2X^3 - 2X^2 + 2X + X^3 - X^2 + X - 1) + 4X^2 - 3X + 1 \\ &= X^5 - 3X^4 + 4X^3 - 4X^2 + 3X + 4X^2 - 3X - 1 + 1 \\ &= X^5 - 3X^4 + 4X^3 \end{aligned}$$

<u>Problem 32:</u> Let X be an n element set. Show that the number of subsets of X with odd number of elements is the same as the number of subsets of X with even number of elements.