Seminar 1

Operation: $* : A \times A \to A$ with $x, y \in A \Rightarrow x * y \in A$.
Grupoid: $(A, *)$
Semigroup: $(A, *)$ grupoid + associativity
Monoid: $(A, *)$ semigroup + identity element
Group: $(A, *)$ monoid + all elements have a simmetric
Abelian group: $(A, *)$ group + commutativity
Subgroupoid = stable part: $\forall a, b \in A \Rightarrow a * b \in A$
Subgroup: $H \leq (G, *)$ if H is a sable part in G ($H \subseteq G$) and $(H, *)$ is a group.

1. Addition: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

   Substraction: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

   Multiplication: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$

   Division: $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$

2. i 3 elements in 3 spaces $\Rightarrow 3^9$

	a	b	c
a			
b			
c			

   ii 3^3 (3 elements in 3 free spaces) and 3^3 (3 commutative elements in 3 spaces) $\Rightarrow 3^6$.

	a	b	c
a		c	b
b	c		a
c	b	a	

   iii 3^4 (3 elemnts in 4 free spaces) and 3 elements, which can be e $\Rightarrow 3^5$

	e	b	c
e	e	b	c
b	b		
c	c		

Generalization:

i n^{n^2}

ii $n^n \cdot n^{\frac{n(n-1)}{2}}$

iii $n^{(n-1)^2+1}$

3. $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+)$ and $(\mathbb{Q}^*,\cdot),(\mathbb{R}^*,\cdot),(\mathbb{C}^*,\cdot)$.

4. i Stable part: $\forall x,y \in \mathbb{R} \Rightarrow x*y = x+y+xy = (x+1)(y+1)-1 \in \mathbb{R}$
Associativity: $\forall x,y \in \mathbb{R} \Rightarrow (x*y)*z = x*(y*z)$
Identity element: $\exists e \in \mathbb{R}$ such that $\forall x \in \mathbb{R} \Rightarrow x*e = e*x = x$
Commutativity: $\forall x,y \in \mathbb{R} \Rightarrow x*y = y*x$.

ii Let A be our interval. Then A is a stable subset of $(\mathbb{R},*)$ $\iff$ $\forall x,y \in A \Rightarrow x*y \in A$.
$x,y \in A \Rightarrow -1 \le x, -1 \le y \Rightarrow 0 \le x+1, 0 \le y+1 \Rightarrow 0 \le (x+1)(y+1) \Rightarrow -1 \le (x+1)(y+1)-1 \Rightarrow x*y \in A$

5. i Here is interesting to see the associativity: $\forall x,y,z \in \mathbb{N} \Rightarrow (x*y)*z = gcd(x,y)*z = gcd(gcd(x,y),z) = \alpha \Rightarrow \alpha \mid gcd(x,y)$ and $\alpha \mid z$. From $gcd(x,y) = d \Rightarrow x = dx_1$ and $y = dy_1$, but $\alpha \mid d \Rightarrow \alpha \mid x$ and $\alpha \mid y \Rightarrow \alpha \mid x,y,z \Rightarrow \alpha \mid gcd(y,z) \Rightarrow \alpha \mid gcd(x, gcd(y,z))$. Analogus for $gcd(x, gcd(y,z)) \mid \alpha$.

ii $\forall x,y \in D_n \Rightarrow x \mid n$ and $y \mid n \Rightarrow n = xd_1$ and $n = yd_2$. We compute $x*y = gcd(x,y) = \alpha \Rightarrow x = \alpha x_1$ and $y = \alpha y_1 \Rightarrow n = \alpha x_1 d_1$ and $n = \alpha y_1 d_2 \Rightarrow \alpha \mid n \Rightarrow gcd(x,y) \mid n \Rightarrow x*y \in D_n$. Associativity, commutativity and identity element are easy to prove.

iii $D_6 = \{1,2,3,6\}$

	1	2	3	6
1	1	1	1	1
2	1	2	1	2
3	1	1	3	3
6	1	2	3	6

6. $H \subseteq \mathbb{Z}$ and H stable part of $\mathbb{Z} \Rightarrow \exists x \in H \Rightarrow \forall n \in \mathbb{N}^*$ we have $x^n \in H$, but H is finite $\Rightarrow \exists n \in \mathbb{N}^*$such that $x^i = x^j, i, j \in \mathbb{N}^*$ and $0 < i < j \Rightarrow x \in \{-1, 0, 1\} \Rightarrow H$ can be $\emptyset, \{0\}, \{1\}, \{0, 1\}, \{-1, 1\}, \{-1, 0, 1\}$.

7. (i) $\Rightarrow$ If G is abelian, then $xy = yx \Rightarrow (xy)^2 = xyxy = xxyy = x^2y^2$. $\Leftarrow \forall x, y \in G : (xy)^2 = x^2y^2 = xxyy$. But $(xy)^2 = xyxy$. So $xyxy = xxyy$. As G is a group, $\exists x^{-1}, y^{-1} \in G$, hence, we multiply with x^{-1} on the left and with y^{-1} on the right and we obtain $yx = xy \Rightarrow G$ is abelian.

   (ii) $\forall x, y \in G : x^2 = 1$ and $y^2 = 1 \Rightarrow x = x^{-1}$ and $y = y^{-1}$, so $xy = x^{-1}y^{-1}$.
   Also, $(xy)^2 = 1 \Rightarrow xy = (xy)^{-1} = y^{-1}x^{-1}$. But $(yx)^2 = 1 \Rightarrow yx = (yx)^{-1} = x^{-1}y^{-1}$.
   Hence, $x^{-1}y^{-1} = y^{-1}x^{-1} \iff xy = yx, \forall x, y \in G$.

8. (i) If $(A, \cdot)$ is a monoid, then $\cdot$ is associative and it has an identity element, let's say $e \in A$.
   Take $X, Y, Z \in P(A) : (X * Y) * Z = \{(xy)z \mid x \in X, y \in Y, z \in Z\} = \{x(yz) \mid x, \in X, y \in Y, z \in Z\} = X * (Y * Z)$. So, $*$ is associative.
   Take $X \in P(A) : X * \{e\} = \{xe \mid x \in X\} = \{ex \mid x \in X\} = \{e\} * X = \{x \mid x \in X\} = X$. So, $*$ has the identity element $\{e\}$.

   (ii) This is easy to see with a counter example.
   If $A = \emptyset$, then $P(A)$ is a group.
   If $A \neq \emptyset$, take $A = \{e\} \Rightarrow P(A) = \{\emptyset, e\}$. We know that the identity element is its own inverse, but $\emptyset$ has no inverse. Hence, $P(A)$ is not a group.

Seminar 2

Homogeneous relation $\varphi : M \to M$.

A graph of a relation φ is a set $A = \{(x, y) \mid x\varphi y\}$, i.e. all the pairs of elements, which are in relation φ with each other. A relation is also given by its graph.

An equivalence relation has to be reflexive (R), transitive (T) and symmetric (S).

R:$\forall x \in A : x\rho x$

T:$\forall x, y, z \in A$ if $x\rho y$ and $y\rho z \Rightarrow x\rho z$

S:$\forall x, y \in A : x\rho y \Rightarrow y\rho x$

We say that $h = (R, M, H)$ is a relation if $H \subseteq R \times M$. And h is a function if $\forall x \in R :\mid h < x >\mid = 1$ (i.e. injective).

We say that $(A_i)_{i\in I}$ is a partition if $\cup_{i\in I} A_i = A$ and $A_i \cap A_j = \emptyset, \forall i, j \in I, i \neq j$.

1. $x \text{ r } y \Rightarrow x < y \Rightarrow R = \{(2, 3), (2, 4), (2, 5), (2, 6), (3, 4), (3, 5), (3, 6), (4, 5), (4, 6), (5, 6)\}$

   $x \text{ s } y \Rightarrow x \mid y \Rightarrow S = \{(2, 4), (2, 6), (3, 6), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6)\}$

   $x \text{ t } y \Rightarrow gcd(x, y) = 1 \Rightarrow T = \{(2, 3), (3, 2), (2, 5), (5, 2), (3, 4), (4, 3), (3, 5), (5, 3), (4, 5),$
   $(5, 4), (5, 6), (6, 5)\}$

   $x \text{ v } y \Rightarrow x \equiv y(mod 3) \Rightarrow V = \{(3, 6), (6, 3), (2, 5), (5, 2), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6)\}$

2. i $\varphi : A \to B \Rightarrow$ Number of $\varphi = 2^{|A\times B|} = 2^{mn}$ Because we have m elements from A, which can form pairs with n elements from B, so mn pair in the end. But those pairs can be written in 2 different ways, like $(a, b), (b, a)$, so it gives us the number stated before.

   ii $\varphi : A \to A \Rightarrow$ Number of $\varphi = 2^{|A\times A|} = 2^{n^2}$

3. $A = \{1, 2, 3\}$

   $R = \{(1, 1), (2, 2), (3, 3)\}$

   $T = \{(1, 2), (2, 3), (1, 3)\}$

   $S = \{(1, 2), (2, 1)\}$

4. $(\mathbb{R}, \neq)$

$$R : \forall x \in \mathbb{R}, x \neq x(false)$$

$(\mathbb{N}, |)$

$$R : \forall x \in \mathbb{N}, x \mid x(true)$$

$$T : \forall x, y, z \in \mathbb{N} y \mid x, z \mid y \Rightarrow z \mid x(true)$$

$$S : \forall x, y \in \mathbb{N}, x \mid y \iff y \mid x(false)$$

The same goes for $(\mathbb{Z}, |)$.

$(V^3, \perp)$

$$R : \forall x \in V^3, x \perp x(false)$$

$(V^3, \|)$

$$R : \forall x \in V^3, x \parallel x(false)$$

$(V^2, \equiv)$

$$R : \forall x \in V^2, x \equiv x(true)$$

$$T : \forall x, y, z \in V^2, x \equiv y, y \equiv z \Rightarrow x \equiv z(true)$$

$$S : \forall x, y \in V^2, x \equiv y \iff y \equiv x(true)$$

$(V^2, \sim)$

$$R : \forall x \in V^2, x \sim x(true)$$

$$T : \forall x, y, z \in V^2, x \sim y, y \sim z \Rightarrow x \sim z(true)$$

$$S : \forall x, y \in V^2, x \sim y \iff y \sim x(true)$$

5. i $R_1 = \{(1,1), (2,2), (3,3), (1,2), (2,1), (1,3), (3,1), (2,3), (3,2), (4,4)\}$. From the pairs $(1,1), (2,2), (3,3), (4,4)$ we can say that R_1 is reflexive. From pairs like $(1,2), (2,1)$ we check that R_1 is symmetric. And from pairs like $(1,2), (2,3), (1,3)$ we check that R_1 is transitive. So r_1 is an equivalence.$\Rightarrow \pi = \{1, 2, 3, 4\}$.

   $R_2 = \{(1,1), (2,2), (3,3), (4,4), (1,2), (1,3)\}$. We check that R_2 is reflexive, transitive, but not symmetric. So r_2 is not an equivalence.

ii For $\pi_1 \Rightarrow \{1\} \cup \{2\} \cup \{3,4\} = \{1,2,3,4\} = M$, $\{1\} \cap \{2\} = \emptyset, \{1\} \cap \{3,4\} = \emptyset, \{2\} \cap \{3,4\} = \emptyset \Rightarrow \pi_1$ is a partition of $M \Rightarrow Gr = \{(1,1),(2,2),(3,3),(3,4),(4,3),(4,4)\}$.

For $\pi_2 \Rightarrow \{1\}\cup\{1,2\}\cup\{3,4\} = \{1,2,3,4\} = M$, but $\{1\}\cap\{1,2\} = \{1\} \neq \emptyset \Rightarrow \pi_2$ is not a partition of M.

6. We check if r is reflexive, transitive and symmetric, which it is, so r is an equivalence relation. We compute $\mathbb{C}/r = \{r(z) \mid z \in \mathbb{C}\} = \{zrz \mid z \in \mathbb{C}\} = \{r(z) \mid\mid z \mid=\mid \overline{z} \mid, z \in \mathbb{C}\} = \{0\} \cup \{C(0, \mid z \mid)\}$.

   We now check the same for s and by simple computations, we get that s is also an equivalence relation. And we compute $\mathbb{C}/s = \{s(z) \mid z \in \mathbb{C}\} = \{zsz \mid arg(z) = arg(\overline{z}), z \in \mathbb{C}\} = \{$ the line starting from $O \mid$ which has the angle $arg(z)$ with $Ox\} \cup \{0\}$.

7.

$$R : \forall x \in \mathbb{Z} : x\rho_n y \Rightarrow n \mid (x-x), (true)$$

$$T : \forall x,y,z \in \mathbb{Z} : x\rho_n y, y\rho_n z \Rightarrow n \mid (x-y), n \mid (y-z) \Rightarrow n \mid [(x-y)+(y-z)] \Rightarrow n \mid (x-z), (true)$$

$$S : \forall x,y \in \mathbb{Z} : x\rho_n y \Rightarrow n \mid (x-y) \iff n \mid (y-x) \Rightarrow y\rho_n x, (true)$$

   So, ρ_n is an equivalence relation.

   $\mathbb{Z}/\rho_0 = \{\{x\} \mid x \in \mathbb{Z}\} \iff 0 \mid x-y \iff x = y$

   $\mathbb{Z}/\rho_1 = \{\mathbb{Z}\} \iff 1 \mid x-y$

   $\mathbb{Z}/\rho_n = \{\hat{0}, \hat{1}, \ldots, \widehat{n-1}\}$

8. From the set $M = \{1,2,3\}$ we can get the partitions: $\{\{1\},\{2\},\{3\}\}, \{\{1,2\},\{3\}\}, \{\{1,3\},\{2\}\}, \{\{2,3\},\{1\}\}, M$. With each partition, we get the graph of a relation. For example, for the first partition, we get $\{(1,1),(2,2),(3,3)\}$. So this can be the equality relation, which is an equivalence relation. And it goes like this for every partition.

9. For h to be a function: $\forall x \in \mathbb{Z}$, we have $\mid h < x >\mid = 1$.

   We know that $h < x >= \{y \in M \mid (x,y) \in \mathbb{Z} \times M\} = \{y \in M \mid \exists z \in \mathbb{Z} : x = 4x + y\}$. So, $y \in M$ is the residue of x divided by 4, which is uniquelly determined.

   Hence, $h < x >$ has exactly one element for each $x \in \mathbb{Z} \Rightarrow h$ is a function.

10. First, we take the relation r:

    We try to see if it is symmetric: $mrn \iff \exists a \in \mathbb{N}$ with $m = 2^a n$. And $nrm \iff \exists b \in \mathbb{N}$ with $n = 2^b m$. This means $m = 2^a 2^b m \Rightarrow 2^{a+b} = 1 \Rightarrow a + b = 0$, where $a, b \in \mathbb{N} \Rightarrow a = b = 0 \Rightarrow m$ must be equal to n. So, it is not symmetric $\Rightarrow$ it is not an equivalence relation.

    Now, we take the relation s.

    It is reflexive, as $msm \iff m = m$.

    It is transitive. From msn and nsq, we get $m = n^2 q$ and $n^2 = q \Rightarrow m = q$ (one of the three happens).

    It is symmetric, as msn and $nsm \Rightarrow$ we get all three to be true. So, it is an equivalence relation.

    One shall verify all cases.

Seminar 3

$(G, *)$ is a group, if $*$ is associative, has identity element and all elements have a symmetric.

$(R, +, \cdot)$ is a ring if $(R, +)$ is an Abelian group, $(R^*, \cdot)$ is a semigroup and distributivity holds.

$(H, +)$ is a subgroup of $(G, +)$ if H is a stable subset $(\forall x, y \in H : x + y \in H)$ of G and $(H, +)$ is also a group. Or, we may also say that $H \neq \emptyset$ and $\forall x, y \in H : x - y \in H$.

$(H, +, \cdot)$ is a subring of $(G, +, \cdot)$ if $H \neq \emptyset$, $\forall x, y \in H : x - y \in H$ and $\forall x, y \in H : x \cdot y \in H$.

$f : (G_1, \circ) \to (G_2, *)$ is a group homomorphism if $\forall x, y \in G_1 \Rightarrow f(x \circ y) = f(x) * f(y)$.

$f : (G_1, \circ) \to (G_2, *)$ is a group isomorphism if f is a group homomorphism and f is also bijective (i.e. f is injective and surjective).

We can say that two groups are isomorphic if there exists a group isomorphism between them, i.e. we find a function between the two groups, which is a group isomorphism.

$(a, n) = 1 \iff ax + ny = 1$

1. To be a group, we have to prove that the operation is associative, has identity element and all elements have a symmetric.

   Associativity: $\forall f_1, f_2, f_3 \in S_M \Rightarrow ((f_1 \circ f_2) \circ f_3)(x) = (f_1 \circ (f_2 \circ f_3))(x)$, for any $x \in M$.

   $((f_1 \circ f_2) \circ f_3)(x) = (f_1 \circ f_2)(f_3(x)) = f_1(f_2(f_3(x))) = (f_1(f_2 \circ f_3))(x) = (f_1 \circ (f_2 \circ f_3))(x)$ (true)

   Identity element: $\exists e \in S_M$ such that $\forall f \in S_M : (e \circ f)(x) = (f \circ e)(x) = f(x), \forall x \in M$. Remember that the elements of S_M are functions. So e also has to be a function. Take the second composition: $(f \circ e)(x) = f(e(x)) = f(x) \Rightarrow e(x) = x$. But this is the identity function $1_M \in S_M$, as 1_M is bijective.

   Symmetric: $\forall f \in S_M, \exists f^{-1} \in S_M$ such that $(f \circ f^{-1})(x) = (f^{-1} \circ f)(x) = 1_M(x)$. As f is a bijective function, i.e. f has an inverse, f^{-1}, which is also bijective. So, each function in S_M has an inverse.

   In the end, $(S_M, \circ)$ is a group.

2. For $(R, +, \cdot)$ to be a ring we have to prove that $(R, +)$ is an Abelian group, $(R^*, \cdot)$ is a semigroup and distributivity holds.

$(R, +)$ **group**: We can easily see that $+$ is associative and commutative. The identity element is $\theta(x) = 0 \in R^M$ and each function $f(x)$ has a symmetric $-f(x)$.

$(R, \cdot)$ **semigroup**: Here, $\cdot$ has to be associative, which can be easily proved.

Distributivity: $\forall f, g, h \in R^M : (f \cdot (g+h))(x) = (f \cdot g)(x) + (f \cdot h)(x)$. And it's true.

So, in the end, $(R^M, +, \cdot)$ is a ring. If R is commutative, then R^M is also commutative and if R has an identity element w.r.t. the second operation, then R^M has also an identity element w.r.t. the second operation, which is different from the one in R. ($\epsilon(x) = 1$ to be precise)

3. Remember: $z \in \mathbb{C} \Rightarrow z = a + bi, a, b \in \mathbb{R} \Rightarrow \mid z \mid = \sqrt{a^2 + b^2}$

   For $(H, \cdot)$ to be a subgroup of $(\mathbb{C}^*, \cdot)$, we have to prove that $H \neq \emptyset$ and $\forall x, y \in H : x \cdot y^{-1} \in H$. (Another way to prove this, is that H is a stable subset of $\mathbb{C}^*$ and $(H, \cdot)$ is a group).

   For $H \neq \emptyset$ we have to find a $z \in H$ such that $\mid z \mid = 1$ (in other words, give me an example of such an element). Take $z = 1 \in H \Rightarrow \mid 1 \mid = 1$ (true).

   Now, $\forall z_1, z_2 \in H : z_1 \cdot z_2^{-1} \in H$. If $z_1, z_2 \in H \Rightarrow \mid z_1 \mid = 1$ and $\mid z_2 \mid = 1$. First, we have to prove that our $z_2^{-1} \in H$,so $z_2^{-1} = \frac{1}{z_2} \Rightarrow \mid z_2^{-1} \mid = \frac{1}{|z_2|} = \frac{1}{1} = 1 \Rightarrow z_2^{-1} \in H$. Now, $z_1 \cdot z_2^{-1} = z_1 \cdot \frac{1}{z_2} = \frac{z_1}{z_2}$ and for it to be in H, its modulus has to be $1 \Rightarrow \mid z_1 \cdot z_2^{-1} \mid = \frac{|z_1|}{|z_2|} = 1 \Rightarrow z_1 \cdot z_2^{-1} \in H$.

   In the end, $(H, \cdot) \leq (\mathbb{C}^*, \cdot)$.

   To prove that $(H, +) \nleq (\mathbb{C}, +)$, we can find an example such that $(H, +)$ is not a stable subset. So, take $z_1 = 1$ and $z_2 = i \Rightarrow \mid z_1 \mid = 1$ and $\mid z_2 \mid = 1$, both in H. But $z_1 + z_2 = 1 + i \Rightarrow \mid z_1 + z_2 \mid = \sqrt{1+1} = \sqrt{2} \notin H$.

4. As before, we prove, first, that $U_n \neq \emptyset$. Take: $z = 1 \in U_n \Rightarrow z^n = 1^n = 1$ (true). Now, $\forall z_1, z_2 \in U_n \Rightarrow z_1^n = 1$ and $z_2^n = 1$, where $z_2^{-1} = \frac{1}{z_2} \in \mathbb{C} \Rightarrow (z_2^{-1})^n = \frac{1}{z_2^n} = \frac{1}{1} = 1$. So, $z_1 \cdot z_2^{-1} = \frac{z_1}{z_2} \Rightarrow (z_1 \cdot z_2^{-1})^n = \frac{z_1^n}{z_2^n} = \frac{1}{1} = 1 \in U_n$.

5. (i) $\forall A, B \in GLn(\mathbb{C}) \Rightarrow det(A) \neq 0$ and $det(B) \neq 0 \Rightarrow det(A) \cdot det(B) \neq 0 \Rightarrow det(A \cdot B) \neq 0 \Rightarrow A \cdot B \in GLn(\mathbb{C})$. So $GLn(\mathbb{C})$ stable subset of $(M_n(\mathbb{C}), \cdot)$.

   (ii) Associativity is easy to prove. The identity element for multiplication of matrices is I_n, with $det(I_n) \neq 0$. For the inverse of a matrix, we know that it exists if the determinant of the matrix is different from 0, which we have. We only need to prove that the inverse of each matrix is also in $GLn(\mathbb{C})$: $det(A \cdot A^{-1}) = det(I_n)$, as $A \cdot A^{-1} = I_n \Rightarrow det(A) \cdot det(A^{-1}) = 1$, but $det(A) \neq 0 \Rightarrow det(A^{-1}) \neq 0 \Rightarrow A^{-1} \in GLn(\mathbb{C})$.

   (iii) We use that $SLn(\mathbb{C})$ has to be a stable subset of $GLn(\mathbb{C})$ and $(SLn(\mathbb{C}), \cdot)$ is also a group. For the first part: $\forall A, B \in SLn(\mathbb{C}) \Rightarrow det(A) = 1$ and $det(B) = 1 \Rightarrow det(A) \cdot det(B) = det(A \cdot B) = 1 \Rightarrow A \cdot B \in SLn(\mathbb{C})$. For the second part, it is easy to prove that multiplication of matrices in $SLn(\mathbb{C})$ is associative, the identity element is I_n and the inverse of each matrix exists and it is also in $SLn(\mathbb{C})$.

6. (i) To show that $(\mathbb{Z}[i], +, \cdot)$ is a subring of $(\mathbb{C}, +, \cdot)$, we will prove that: $\mid \mathbb{Z}[i] \mid \geq 2$, $\forall x, y \in \mathbb{Z}[i] : x - y \in \mathbb{Z}[i]$ and $\forall x, y \in \mathbb{Z}[i] : x \cdot y \in \mathbb{Z}[i]$. To prove that we have at least two elements in $\mathbb{Z}[i]$, we have to give examples: $0 = 0 + 0i$ and $1 = 1 + 0i$ are both in $\mathbb{Z}[i]$.

   The second part: $\forall x, y \in \mathbb{Z}[i] \Rightarrow x = a_1 + b_1 i$ and $y = a_2 + b_2 i$, where $-y = -a_2 - b_2 i \in \mathbb{Z}[i] \Rightarrow x - y = (a_1 - a_2) + (b_1 - b_2)i \in \mathbb{Z}[i]$, as $a_1 - a_2 \in \mathbb{Z}$ and $b_1 - b_2 \in \mathbb{Z}$.

   Finally, we have: $x \cdot y = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2)i \in \mathbb{Z}[i]$, as $a_1 a_2 - b_1 b_2 \in \mathbb{Z}$ and $a_1 b_2 + b_1 a_2 \in \mathbb{Z}$.

   So $(\mathbb{Z}[i], +, \cdot)$ is a subring of $(\mathbb{C}, +, \cdot)$.

   (ii) Here, we use the same thing. So, for M to have at least two elements, we find the matrices $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in M$. Then $\forall A, B \in M \Rightarrow A = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}$ and $B = \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix} \Rightarrow A - B = \begin{bmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & c_1 - c_2 \end{bmatrix} \in M$, as $a_1 - a_2, b_1 - b_2, c_1 - c_2 \in \mathbb{R}$. And $A \cdot B = \begin{bmatrix} a_1 a_2 & a_1 b_2 + b_1 c_2 \\ 0 & c_1 c_2 \end{bmatrix} \in M$, as $a_1 a_2, a_1 b_2 + b_1 c_2, c_1 c_2 \in \mathbb{R}$. So, $(M, +, \cdot)$ is a subring of $(M_2(\mathbb{R}), +, \cdot)$.

7. (i) For f to be a group homomorphism, we have to prove that: $\forall z_1, z_2 \in \mathbb{C}^* \Rightarrow f(z_1 \cdot z_2) = f(z_1) \cdot f(z_2)$.
So, $f(z_1 \cdot z_2) = \mid z_1 \cdot z_2 \mid = \mid z_1 \mid \cdot \mid z_2 \mid = f(z_1) \cdot f(z_2)$ (true).
(ii) The same things go for g: $\forall z_1, z_2 \in \mathbb{C}^* \Rightarrow z_1 = a_1 + b_1 i$ and $z_2 = a_2 + b_2 i$.

$$g(z_1 \cdot z_2) = g(a_1a_2 - b_1b_2 + i(a_1b_2 + a_2b_1)) = \begin{bmatrix} a_1a_2 - b_1b_2 & a_1b_2 + a_2b_1 \\ -a_1b_2 - a_2b_1 & a_1a_2 - b_1b_2 \end{bmatrix}$$

$$g(z_1) \cdot g(z_2) = \begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 - b_1b_2 & a_1b_2 + a_2b_1 \\ -a_1b_2 - a_2b_1 & a_1a_2 - b_1b_2 \end{bmatrix}$$

So, $g(z_1 \cdot z_2) = g(z_1) \cdot g(z_2) \Rightarrow g$ is a group homomorphism.

8. For $(\mathbb{Z}_n, +)$ to be isomorphic with $(U_n, \cdot)$, we have to find a function between them, which is a group isomomorphism.

Take, $f : U_n \to \mathbb{Z}_n$, such that $f(z^k) = k, \forall k \in \mathbb{Z}_n$. We can easily see that f is a group homomorphism, as $f(z^{k_1} \cdot z^{k_2}) = f(z^{k_1+k_2}) = k_1 + k_2 = f(z^{k_1}) + f(z^{k_2})$. And also, f is a bijetive function.

Pay attention to the case: $k = n$, where $n \in \mathbb{Z}_n$ is $0 \Rightarrow f(z^n) = f(1) = 0 = n \in \mathbb{Z}_n$.

9. (i) $\hat{a}$ invertible $\in \mathbb{Z}_n^* \iff \exists \hat{b} \in \mathbb{Z}_n^*$ such that $\hat{a}\hat{b} = \hat{1} \iff \widehat{ab} = \hat{1} \iff n \mid ab - 1 \iff \exists k \in \mathbb{Z}$ such that $ab - 1 = nk \iff a \cdot b + n \cdot (-k) = 1 \iff (a, n) = 1$.
(ii) $\mathbb{Z}_n$ field $\iff \forall \hat{a} \in \mathbb{Z}_n$ is invertible $\iff \hat{1}, \hat{2}, \ldots, \widehat{n-1}$ are invertible. From (i) $\Rightarrow (1, n) = 1, (2, n) = 1, \ldots, (n-1, n) = 1 \Rightarrow n$ is prime.

10. Let $f : \mathbb{C} \to M$ with $f(a + bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$.

First, we need to prove that $(M, +, \cdot)$ is a field, which is easy. $(M, +)$ is an abelian group, as addition of matrices is associative and commutative (we know), the identity element is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in M$ and the symmetric elements are $\begin{bmatrix} -a & -b \\ b & -a \end{bmatrix} \in M$.

Also, $(M^*, \cdot)$ is a group, as multiplication of matrices is associative, the identity element is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in M^*$ and all the elements are invertible, as $det(A) = a^2 + b^2 \geq 0$, but $A \neq O_2$, so $a \neq 0$ or $b \neq 0 \Rightarrow det(A) \neq 0 \iff A$ invertible.

And distributivity holds.

For f to be an isomorphism, f must be a bijective homomorphism.

$\forall a + bi, c + di \in \mathbb{C} \Rightarrow f((a + bi) + (c + di)) = f((a + c) + i(b + d)) = \begin{bmatrix} a + c & b + d \\ -(b + d) & a + c \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = f(a + bi) + f(c + di)$.

$\forall a + bi, c + di \in \mathbb{C} \Rightarrow f((a + bi) \cdot (c + di)) = f((ac - bd) + i(ad + bc)) = \begin{bmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{bmatrix}$. And $f(a+bi) \cdot f(c+di) = \begin{bmatrix} ac - bd & ad + bc \\ -bc - ad & ac - bd \end{bmatrix}$. So, they are equal $\Rightarrow f$ is an homomorphism.

It is easy to see that f is bijective, as $\exists! \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ such that we have $f(a + bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$.

In the end, f is a field isomorphism.

Seminar 4

Let $(K, *, \circ)$ be a field, then we define the operation between a scalar from K and a vector from V such that $\forall k \in K$ and $\forall v \in V$ we have $k \cup v \in V$. Then V is a **vector space** if $(V, \perp)$ is an Abelian group (where $\perp$ is the operation between vectors) and:

a $k \cup (v_1 \perp v_2) = k \cup v_1 \perp k \cup v_2$

b $(k_1 * k_2) \cup v = k_1 \cup v \perp k_2 \cup v$

c $(k_1 \circ k_2) \cup v = k_1 \cup (k_2 \cup v)$

d $e \cup v = v$, where e is the identity element.

But for a vector space, please remember that we talk about the operations on vectors and multiplication with scalars.

S is a **subspace** of V if: S is a stable subset and S is a vector space with respect to the same operation. We may also say that S is a subspace of V if $\forall k_1, k_2 \in K$ and $\forall x, y \in S \Rightarrow S \neq \emptyset$ and $k_1x + k_2y \in S$.

1. a $k(f_1 + f_2) = k[a_{10} + a_{20} + (a_{11} + a_{21})X + \cdots + (a_{1n} + a_{2n})X^n] = ka_{10} + ka_{11}X + \cdots + ka_{1n}X^n + ka_{20} + \cdots + ka_{2n}X^n = kf_1 + kf_2$

   b $(k_1 + k_2)f = (k_1 + k_2)a_0 + (k_1 + k_2)a_1X + \cdots + (k_1 + k_2)a_nX^n = k_1a_0 + k_1a_1X + \cdots + k_1a_nX^n + k_2a_0 + \cdots + k_2a_nX^n = k_1f + k_2f$

   c $(k_1k_2)f = k_1k_2a_0 + k_1k_2a_1X + \cdots + k_1k_2a_nX^n = k_1(k_2a_0 + k_2a_1X + \cdots + k_2a_nX^n) = k_1(k_2f)$

   d $1 \cdot f = 1 \cdot (a_0 + a_1X + \cdots + a_nX^n) = a_0 + a_1X + \cdots + a_nX^n = f$

2. a $\alpha(A + B) = \alpha A + \alpha B$

   b $(\alpha + \beta)A = (\alpha + \beta) = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} = \alpha A + \beta A$

   c $(\alpha\beta)A = \begin{bmatrix} \alpha\beta a_{11} & \dots & \alpha\beta a_{1n} \\ \dots & \dots & \dots \\ \alpha\beta a_{m1} & \dots & \alpha\beta a_{mn} \end{bmatrix} = \alpha \begin{bmatrix} \beta a_{11} & \dots & \beta a_{1n} \\ \dots & \dots & \dots \\ \beta a_{m1} & \dots & \beta a_{mn} \end{bmatrix} = \alpha(\beta A)$

   d $1 \cdot A = 1 \cdot \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} = A$

3. a $\forall x \in A : [k(f+g)](x) = k(f(x)+g(x)) = kf(x)+kg(x)$
   b $\forall x \in A : [(k_1+k_2)f](x) = (k_1+k_2)f(x) = k_1 f(x) + k_2 f(x)$
   c $[(k_1 \cdot k_2)f](x) = (k_1 \cdot k_2)f(x) = k_1 k_2 f(x) = [k_1(k_2 f)](x)$
   d $(1 \cdot f)(x) = 1 \cdot f(x) = f(x)$

   So, $\forall A \neq \emptyset$ and $\forall K$-field $\Rightarrow K^A$ is a vector space. Now, take $A = \mathbb{R} \neq \emptyset$ and $\mathbb{R}$ is a field $\Rightarrow \mathbb{R}^{\mathbb{R}}$ is a vector space.

4. a $kT(x \perp y) = kT(xy) = (xy)^k = x^k y^k = (kTx)(kTy) = (kTx) \perp (kTy)$
   b $(k_1+k_2)Tx = x^{k_1+k_2} = x^{k_1} \cdot x^{k_2} = (k_1 Tx) \perp (k_2 Tx)$
   c $(k_1 \cdot k_2)Tx = x^{k_1 \cdot k_2} = (x^{k_2})^{k_1} = k_1 T(k_2 Tx)$
   d $1Tx = x^1 = x$

   $\Rightarrow$ is a vector space.

5. (i) We have a problem at $(k_1+k_2)v = k_1 v + k_2 v$, as $(k_1+k_2)v = ((k_1+k2)x, y)$, but $k_1 v + k_2 v = ((k_1+k_2)x, y+2y)$, which are not equal. Hence, it is not a K-vector space.
   (ii) The same problem we have here, as $(k_1+k_2)v = ((k_1+k_2)x, y)$, but $k_1 v + k_2 v = ((k_1+k_2)x, y+y)$, which again are not equal. Hence, this is not a K-vector space.

6. (i) As V is a $\mathbb{Z}_p$-vector space, we have the scalars from $\mathbb{Z}_p$.
   We use the properties of a vector space:

$$\hat{1} \cdot x = x$$

$$\hat{1}x + \hat{1}x = (\hat{1}+\hat{1})x = \hat{2}x$$
$$\hat{1}x + \hat{2}x = (\hat{1}+\hat{2})x = \hat{3}x$$
$$\dots$$
$$\hat{1}x + \dots \hat{1}x = \hat{p}x = \hat{0}x = \hat{0} = 0$$

   (ii) Homework

7. For this exercise we will use that S is a subspace of V if $S \neq \emptyset$ and $\forall k_1, k_2 \in K$ and $\forall x, y \in S$, we have $k_1 x + k_2 y \in S$.

(i) $\forall \alpha, \beta \in \mathbb{R}, \forall (0, y_1, z_1), (0, y_2, z_2) \in A \Rightarrow \alpha(0, y_1, z_1) + \beta(0, y_2, z_2) = (0, \alpha y_1 + \beta y_2, \alpha z_1 + \beta z_2) \in A \Rightarrow A$ is a subspace of $\mathbb{R}^3$.

(ii) $\forall \alpha, \beta \in \mathbb{R}, \forall (x_1, y_1, z_1), (x_2, y_2, z_2) \in B$.
If $x_1 = x_2 = 0 \Rightarrow B$ is a subspace of $\mathbb{R}^3$.
If $z_1 = z_2 = 0 \Rightarrow B$ is a subspace of $\mathbb{R}^3$.
If $x_1 = z_2 = 0 \Rightarrow \alpha(0, y_1, z_1) + \beta(x_2, y_2, 0) = (\beta x_2, \alpha y_1 + \beta y_2, \alpha z_1) \notin B \Rightarrow B$ is NOT a subspace of $\mathbb{R}^3$.

(iii) $\forall \alpha, \beta \in \mathbb{R}, \forall (x_1, y_1, z_1), (x_2, y_2, z_2) \in C \Rightarrow \alpha(x_1, y_1, z_1) + \beta(x_2, y_2, z_2) \notin C$, as $x_1, x_2 \in \mathbb{Z}$ and $\alpha, \beta \in \mathbb{R}$, but $\alpha x_1, \beta x_2 \in \mathbb{R}$, when they should be in $\mathbb{Z} \Rightarrow C$ is NOT a subspace of $\mathbb{R}^3$. If $\alpha, \beta \in \mathbb{Z} \Rightarrow C$ is a subspace.

(iv) $\forall \alpha, \beta \in \mathbb{R}, \forall (x_1, y_1, z_1), (x_2, y_2, z_2) \in D \Rightarrow \alpha(x_1, y_1, z_1) + \beta(x_2, y_2, z_2) = (\alpha x_1 + \beta x_2, \alpha y_1 + \beta y_2, \alpha z_1 + \beta z_2) \in D$, as $x_1 + y_1 + z_1 = 0 \Rightarrow \alpha x_1 + \alpha y_2 + \alpha z_1 = 0$ (the same for β) and so $\alpha x_1 + \beta x_2 + \alpha y_1 + \beta y_2 + \alpha z_1 + \beta z_2 = 0$.

(v) $\forall \alpha, \beta \in \mathbb{R}, \forall (x_1, y_1, z_1), (x_2, y_2, z_2) \in E \Rightarrow \alpha(x_1, y_1, z_1) + \beta(x_2, y_2, z_2) = (\alpha x_1 + \beta x_2, \alpha y_1 + \beta y_2, \alpha z_1 + \beta z_2) \notin E$, as $x_1 + y_1 + z_1 = 1 \Rightarrow \alpha x_1 + \alpha y_1 + \alpha z_1 = \alpha$ (the same goes for β), so $\alpha x_1 + \beta x_2 + \alpha y_1 + \beta y_2 + \alpha z_1 + \beta z_2 = \alpha + \beta \neq 1 \Rightarrow E$ is NOT a subspace.

(vi) $\forall \alpha, \beta \in \mathbb{R}, \forall (x_1, x_1, x_1), (x_2, x_2, x_2) \in F \Rightarrow \alpha(x_1, x_1, x_1) + \beta(x_2, x_2, x_2) = (\alpha x_1 + \beta x_2, \alpha x_1 + \beta x_2, \alpha x_1 + \beta x_2) \in F \Rightarrow F$ is a subspace.

8. (i) $\forall x, y \in [-1, 1] \Rightarrow -1 \leq x \leq 1$ and $-1 \leq y \leq 1$. Now, multiply those with $\alpha, \beta \in \mathbb{R} \Rightarrow -\alpha \leq \alpha x \leq \alpha$ and $-\beta \leq \beta y \leq \beta \Rightarrow -\alpha - \beta \leq \alpha x + \beta y \leq \alpha + \beta \Rightarrow [-\alpha - \beta, \alpha + \beta] \neq [-1, 1]$. So $[-1, 1]$ is NOT a subpace of $\mathbb{R}$.

(ii) Take $(1, 0), (0, 1)$ in our set. Then $(1, 0) + (0, 1) = (1, 1)$ is not in our set, as $1^2 + 1^2 = 2 \leq 1$ is not true. $\Rightarrow A$ is NOT a subspace of $\mathbb{R}^2$.

(iii) $\alpha \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} + \beta \begin{bmatrix} d & e \\ 0 & f \end{bmatrix} = \begin{bmatrix} \alpha a + \beta d & \alpha b + \beta e \\ 0 & \alpha c + \beta f \end{bmatrix}$. If $a, d \in \mathbb{Q}$ and $\alpha, \beta \in \mathbb{Q} \Rightarrow \alpha a + \beta d \in \mathbb{Q}$ (analogues for the others) $\Rightarrow B$ is a subspace of $M_2(\mathbb{Q})$. If $a, d \in \mathbb{Q}$ and $\alpha, \beta \in \mathbb{R} \Rightarrow \alpha a + \beta d \in \mathbb{R}$ (Analogues for the others) $\Rightarrow B$ is NOT a subspace of $M_2(\mathbb{R})$.

(iv) $\alpha f_1 + \beta f_2$ is continuous, as f_1, f_2 continuous $\Rightarrow$ our set is a subspace of $\mathbb{R}^{\mathbb{R}}$.

9. (i) Take $k, l \leq n$ and $f = a_0 + a_1X + \cdots + a_kX^k, g = b_0 + b_1X + \cdots + b_lX^l$. Suppose $k < l$ and take $\alpha, \beta \in K$. Then $\alpha f + \beta g = (\alpha a_0 + \beta b_0) + \ldots (\alpha a_k + \beta b_k)X^k + \cdots + \beta b_l X^l \Rightarrow degree(\alpha f + \beta g) = l \leq n$, so our set is a subspace.

   (ii) Take $\alpha, \beta \in K$ and $f = a_0 + a_1X + \ldots a_nX^n, g = b_0 + b_1X + \cdots + b_nX^n \Rightarrow \alpha f + \beta g = (\alpha a_0 + \beta b_0) + \cdots + (\alpha a_n + \beta b_n)X^n \Rightarrow degree(\alpha f + \beta g) \leq n \Rightarrow$ our set is NOT a subspace.

10. $S = \{(x_1, x_2) \mid (x_1, x_2)$ - system solutions $\} \Rightarrow S \neq \emptyset$, as $(0, 0)$ is a solution for our system. Now, take $(x_1, x_2), (y_1, y_2) \in S$ and $\alpha, \beta \in K \Rightarrow \alpha(x_1, x_2) + \beta(y_1, y_2) = (\alpha x_1 + \beta y_1, \alpha x_2 + \beta y_2)$ should be a solution $\iff a_{11}(\alpha x_1 + \beta y_1) + a_{12}(\alpha x_2 + \beta y_2) = \alpha(a_{11}x_1 + a_{12}x_2) + \beta(a_{11}y_1 + a_{22}y_2) = 0$, as $a_{11}x_1 + a_{12}x_2 = 0$ ((x_1, x_2) is a solution). And the same goes for the other equation $\Rightarrow S$ is a subspace for $\mathbb{R}^2$.

Seminar 5

$V = A \oplus B$ if $V = A + B$ and $A \cap B = \{0\}$. Or $\forall v \in V, \exists! s \in S, t \in T$ such that $v = s + t$.

$f : A \to B$ **endomorphism** if $A = B$ and f homomorphism.

$ker(f) = \{x \in R \mid f(x) = 0\}$ and $Im(f) = \{f(x) \mid x \in R\}$.

1. (i) $< 1, X, X^2 >= \{a + bX + cX^2 \mid a, b, c \in \mathbb{R}\} = \mathbb{R}_2[X]$.

   (ii) $< \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} >=$
   $\{a \cdot \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + b \cdot \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + c \cdot \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + d \cdot \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \mid a, b, c, d \in \mathbb{R}\} =$
   $\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R}\} = M_2(\mathbb{R})$.

2. (i) $(0, a, b) = (0, a, 0) + (0, 0, b) = a \cdot (0, 1, 0) + b \cdot (0, 0, 1) \Rightarrow$
   $A =< (0, 1, 0), (0, 0, 1) >$.

   (ii) $a + b + c = 0 \Rightarrow a = -b - c = -(b + c) \Rightarrow (-(b + c), b, c) = (-b, b, -0) + (-c, 0, c) = b(-1, 1, 0) + c(-1, 0, 1) \Rightarrow B =< (-1, 1, 0), (-1, 0, 1) >$.

   (iii) $(a, a, a) = a(1, 1, 1) \Rightarrow C =< (1, 1, 1) >$.

3. In order for those two to be equal, we may show that, for example, the vectors c, d, e can be written as a linear combination of the vectors a, b.

   It is easy to see that: $\begin{cases} c = a + b \\ d = a - b \\ e = 3a - b \end{cases}$

4. $S =< (-1, 1, 0), (-1, 0, 1) >\Rightarrow s_1 = (-1, 1, 0)$ and $s_2 = (-1, 0, 1)$.

   $T =< (1, 1, 1) >\Rightarrow t = (1, 1, 1)$.

   From *Seminar4*, we know that S, T are subspaces of $\mathbb{R}^{\mathbb{R}}$. To prove that $\mathbb{R}^3 = S \oplus T$, we prove that $S + T = \mathbb{R}^3$ and $S \cap T = \{0_3\}$.

   $\forall v \in \mathbb{R}^3, \exists! s \in S, \exists! t \in T$ such that $v = s + t \iff (v_1, v_2, v_3) = a \cdot s_1 + b \cdot s_2 + c \cdot t \iff (v_1, v_2, v_3) = (-a, a, 0) + (-b, 0, b) + (c, c, c) \iff$

   $\begin{cases} v_1 = -a - b + c \\ v_2 = a + c \\ v_3 = b + c \end{cases} \Rightarrow \begin{cases} a = -\frac{1}{3}v_1 + \frac{2}{3}v_2 - \frac{1}{3}v_3, \\ b = -\frac{1}{3}v_1 - \frac{1}{3}v_2 + \frac{2}{3}v_3 \\ c = \frac{1}{3}(v_1 + v_2 + v_3) \end{cases}$, so they are unique.

5. Remember:

$$f : \mathbb{R} \to \mathbb{R},\ \text{f-odd} \Rightarrow \forall x \in \mathbb{R}, f(-x) = -f(x)$$

$$f : \mathbb{R} \to \mathbb{R},\ \text{f-even} \Rightarrow f(-x) = f(x)$$

.

$S \neq \emptyset$, as $\theta(x) = 0 \in S$ and $t \neq \emptyset$, as $f(x) = -x \in T$.

Take $f, g \in S, a, b \in \mathbb{R} \Rightarrow (af + bg)(-x) = (af)(-x) + (bg)(-x) = -af(x) - bg(x) = -(af + bg)(x) \in S \Rightarrow S \leq \mathbb{R}^{\mathbb{R}}$.

Take $f, g \in T, a, b \in \mathbb{R} \Rightarrow (af + bg)(-x) = (af)(-x) + (bg)(-x) = af(x) + bg(x) = (af + bg)(x) \in T \Rightarrow T \leq \mathbb{R}^{\mathbb{R}}$.

Take $f : \mathbb{R} \to \mathbb{R}, g \in S, h \in T$, as $f(x) = g(x) + h(x)$. Then $f(-x) = g(-x) + h(-x) = -g(x) + h(x) \Rightarrow g(x) = \frac{1}{2}(f(x) + f(-x)) \in S$ and $h(x) = \frac{1}{2}(f(x) - f(-x)) \in R$. So, g, h are unique functions, with which we can write any function $f : \mathbb{R} \to \mathbb{R}$. Now, for the intersection: if $f(-x) = -f(x)$ and $f(-x) = f(x) \Rightarrow f(x) = -f(x) \Rightarrow f(x) = \theta(x)$. So $S \cap T = \{\theta(x) = 0\}$.

6. $f((x_1, y_1) + (x_2, y_2)) = f(x_1 + x_2, y_1 + y_2) = (x_1 + x_2 + y_1 + y_2, x_1 + x_2 - y_1 - y_2) = (x_1 + y_1, x_1 - y_1) + (x_2 + y_2, x_2 - y_2) = f(x_1, y_1) + f(x_2, y_2)$

$f(k(x, y)) = f(kx, ky) = (kx + ky, kx - ky) = (k(x + y), k(x - y)) = k(x + y, x - y) = kf(x, y)$

$\Rightarrow f$ endomorphism.

$g((x_1, y_1) + (x_2, y_2)) = g(x_1 + x_2, y_1 + y_2) = (2x_1 + 2x_2 - y_1 - y_2, 4x_1 + 4x_2 - 2y_1 - 2y_2) = g(x_1, y_1) + g(x_2, y_2)$

$g(k(x, y)) = (2kx - ky, 4kx - 2ky) = (k(2x - y), k(4x - 2y)) = kg(x, y)$

$\Rightarrow g$ endomorphism.

$h((x_1, y_1, z_1) + (x_2, y_2, z_2)) = h(x_1 + x_2, y_1 + y_2, z_1 + z_2) = (x_1 + x_2 - y_1 - y_2, y_1 + y_2 - z_1 - z_2, z_1 + z_2 - x_1 - x_2) = h(x_1, y_1, z_1) + h(x_2, y_2, z_2)$

$h(k(x, y)) = (kx - ky, ky - kz, kz - kx) = (k(x - y), k(y - z), k(z - x)) = kh(x, y, z)$

$\Rightarrow h$ endomorphism.

7. (i) $f(x, y) = (ax + by, cx + dy)$

$f(x_1 + x_2, y_1 + y_2) = (ax_1 + ax_2 + by_1 + by_2, cx_1 + cx_2 + dy_1 + dy_2) = (ax_1 + by_1, cx_1 + dy_1) + (ax_2 + by_2, cx_2 + dy_2) = f(x_1, y_1) + f(x_2, y_2)$

$f(k(x,y)) = (kax+kby, kcx+kdy) = k(ax+by, cx+dy) = kf(x,y)$
$\Rightarrow f$ endomorphism.

(ii) $g(x,y) = (a+x, b+y)$
For $a = b = 0 \Rightarrow g(x,y) = (x,y)$ - endomorphism of $\mathbb{R}^2$. But $\forall a,b \in \mathbb{R}^* \Rightarrow g(x_1+x_2, y_1+y_2) = (a+x_1+x_2, b+y_1+y_2) = (a+x_1, b+y_1) + (x_2, y_2) = g(x_1,y_1) + (x_2,y_2) \Rightarrow g$ is NOT an endomorphism.

8. $\forall (x,y), (m,n) \in \mathbb{R}^2, \forall k \in \mathbb{R}$ we have:

$$f((x,y)+(m,n)) = f(x+m, y+n) = f(x,y) + f(m,n)$$

$$f(k(x,y)) = f(kx, ky) = kf(x,y)$$

(Homework)

9. $ker(f) = \{(x,y) \mid (x+y, x-y) = (0,0)\} \Rightarrow x+y = 0$ and $x-y = 0 \Rightarrow x = y$ and $2y = 0 \Rightarrow x = y = 0 \Rightarrow ker(f) = \{(0,0)\}$.

$Im(f) = \{(x+y, x-y) \mid x,y \in \mathbb{R}\} = \{(x,x)+(y,-y) \mid x,y \in \mathbb{R}\} = \{x(1,1)+y(1,-1) \mid x,y \in \mathbb{R}\} \Rightarrow Im(f) =< (1,1), (1,-1) >$.

$ker(g) = \{(x,y) \mid (2x-y, 4x-2y) = (0,0)\} \Rightarrow 2x-y = 0$ and $4x-2y = 0 \Rightarrow 2x = y$. So, take $x = a \in \mathbb{R} \Rightarrow y = 2a \in \mathbb{R} \Rightarrow ker(g) = \{(a,2a) \mid a \in \mathbb{R}\} =< (1,2) >$

$Im(g) = \{(2a-b, 4a-2b) \mid x,y \in \mathbb{R}\} = \{(2a,4a)+(-b,-2b) \mid x,y \in \mathbb{R}\} = \{a(2,4)+b(-1,-2) \mid x,y \in \mathbb{R}\} \Rightarrow Im(g) =< (2,4), (-1,-2) >$

$ker(h) = \{(x,y,z) \mid (x-y, y-z, z-x) = (0,0,0)\} \Rightarrow x-y = 0, y-z = 0, z-x = 0 \Rightarrow x = y = z \Rightarrow ker(h) = \{(x,x,x) \mid x \in \mathbb{R}\} =< (1,1,1) >$

$Im(h) = \{(a-b, b-c, c-a) \mid a,b,c \in \mathbb{R}\} = \{(a,0,a)+(-b,b,0)+(0,-c,c) \mid a,b,c \in \mathbb{R}\} = \{a(1,0,-1)+b(-1,1,0)+c(0,-1,1) \mid a,b,c \in \mathbb{R}\} \Rightarrow Im(h) =< (1,0,-1), (-1,1,0), (0,-1,1) >$.

10. $S \neq \emptyset$, as $f(0) = 0 \in S$.

$\forall x,y \in S \Rightarrow x+y = f(x)+f(y) = f(x+y) \in S$, as f is an endomorphism.

$\forall a \in K, \forall x \in S \Rightarrow ax = af(x) = f(ax) \in S$, as f is an endomorphism.

So, $S \leq V$.

Seminar 6

We say that $v_1, v_2, \dots v_n$ are **linearly independent** if

$$a_1v_1 + a_2v_2 + \dots a_nv_n = 0 \iff a_1 = a_2 = \dots = a_n = 0$$

or if the determinant, given by the vectors written on lines, is different from zero.

We say that B is a **basis** if the vectors in B are linearly independent and the vectors in B generate the whole space.

1. (i) $a_1v_1 + a_2v_2 + a_3v_3 = 0 \iff \begin{cases} a_1 + 2a_2 + a_3 = 0 \\ a_1 + a_2 + 5a_3 = 0 \\ a_2 + 2a_3 = 0 \end{cases}$
   From the last equation we have $a_2 = -2a_3$ so our system becomes $\begin{cases} a_1 - 4a_3 + a_3 = 0 \\ -a_1 - 2a_3 + 5a_3 = 0 \end{cases} \Rightarrow a_1 - 3a_3 = 0 \Rightarrow a_1 = 3a_3 \Rightarrow S = \{(3a, -2a, a) \mid a \in \mathbb{R}\} \Rightarrow v_1, v_2, v_3$ are linearly dependent.

   (ii) $a_1v_1 + a_2v_2 = 0 \iff \begin{cases} a_1 + 2a_2 = 0 \\ -a_1 + a_2 = 0 \\ a_2 = 0 \end{cases} \Rightarrow a_1 = 0 \Rightarrow v_1, v_2$ are linearly independent.

2. (i) $a_1v_1 + a_2v_2 + a_3v_3 = 0 \iff \begin{cases} a_1 - a_2 + 3a_3 = 0 \\ 2a_2 + a_3 = 0 \\ 2a_1 + a_2 + a_3 = 0 \end{cases} \Rightarrow$ By simple computations we get that $a_1 = a_2 = a_3 = 0 \Rightarrow v_1, v_2, v_3$ are linearly independent.

   (ii) $\begin{vmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{vmatrix} = \begin{vmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{vmatrix} = -192 \neq 0 \Rightarrow v_1, v_2, v_3, v_4$ are linearly independent.

3. $\begin{vmatrix} 1 & a & 0 \\ a & 1 & 1 \\ 1 & 0 & a \end{vmatrix} = a(\sqrt{2} - a)(\sqrt{2} + a) = 0$ (if this is 0, the vectors are dependent, if not, they are independent) $\Rightarrow a = 0$ or $a = \sqrt{2}$ or $a = -\sqrt{2} \Rightarrow$ for v_1, v_2, v_3 to be linearly independet $a \in \mathbb{R} \setminus \{-\sqrt{2}, 0, \sqrt{2}\}$.

4. $a_1v_1+a_2v_2+a_3v_3 = 0 \iff \begin{cases} a_1 + 2a_2 = 0 \\ -2a_1 + a_2 + aa_3 = 0 \\ a_2 + a_3 = 0 \\ -a_1 + 2a_3 = 0 \end{cases} \Rightarrow \begin{cases} a_2 = -a_3 \\ a_1 = 2a_3 \\ -4a_3 - a_3 + aa_3 = 0 \end{cases} \Rightarrow$ $(a-5)a_3 = 0 \Rightarrow a \in \mathbb{R} \setminus \{5\}$. (Here, a_3 could not be 0, as all of them would have been 0, which means that the vectors would have been linearly independent).

5. (i) $\begin{vmatrix} 1 & 1 & 0 \\ -1 & 0 & 2 \\ 1 & 1 & 1 \end{vmatrix} = 1 \neq 0 \Rightarrow (v_1, v_2, v_3)$ linealry independent.
$\forall u = (u_1, u_2, u_3) \in \mathbb{R}^3, \exists! a_1, a_2, a_3 \in \mathbb{R}$ such that

$$a_1v_1 + a_2v_2 + a_3v_3 = u \Rightarrow \begin{cases} a_1 - a_2 + a_3 = u_1 \\ a_1 + a_3 = u_2 \\ 2a_2 + a_3 = u_3 \end{cases} \Rightarrow$$

By simple computations we get that $\begin{cases} a_1 = 3u_2 - u_3 - 2u1 \\ a_2 = u_2 - u_1 \\ a_3 = u_3 - 2u_2 + 2u_1 \end{cases} \Rightarrow$ (v_1, v_2, v_3) generates $\mathbb{R}^3 \Rightarrow (v_1, v_2, v_3)$ is a basis.

(ii) We have to solve all three systems $a_1v_1 + a_2v_2 + a_3v_3 = e_1$ and $a_1v_1 + a_2v_2 + a_3v_3 = e_2$ and $a_1v_1 + a_2v_2 + a_3v_3 = e_3$. In other words, to find a_1, a_2, a_3 in each case. $\Rightarrow \begin{cases} e_1 = 2v_1 + v_2 - 2v_3 \\ e_2 = 3v_1 + v_2 - 2v_3 \\ e_3 = -v_1 + v_3 \end{cases}$

(iii) In (e_1, e_2, e_3) we have the coordinates for u as $(1, -1, 2)$. So, $a_1v_1 + a_2v_2 + a_3v_3 = (1, -1, 2)$, and by solving the system, we find $a_1 = -7, a_2 = -2, a_3 = 6 \Rightarrow$ In the basis (v_1, v_2, v_3), u has the coordinates $(-7, -2, 6)$.

6.

$$\Delta = \begin{vmatrix} 1 & 1 & \dots & 1 & 1 & 1 \\ 1 & 1 & \dots & 1 & 1 & 2 \\ 1 & 1 & \dots & 1 & 2 & 3 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & 2 & \dots & n-2 & n-1 & n \end{vmatrix}$$

$$= (-1)^{n+1}\cdot 1\cdot \begin{vmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 2 \\ \dots & \dots & \dots & \dots \\ 1 & 2 & \dots & n-1 \end{vmatrix} + (-1)^{n+2}\cdot 2\cdot \begin{vmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 2 \\ \dots & \dots & \dots & \dots \\ 1 & 2 & \dots & n-1 \end{vmatrix}$$

$$+(-1)^{n+3}\cdot 3\cdot \begin{vmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots \\ 1 & 2 & \dots & n-1 \end{vmatrix} + \dots + (-1)^{n+n}\cdot n\cdot \begin{vmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots \\ 1 & 2 & \dots & n-2 \end{vmatrix}$$

All of them are zero, as two lines are equal, except the first two determinants.

$$(-1)^{n+1}(1-2)\cdot \begin{vmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 2 \\ \dots & \dots & \dots & \dots \\ 1 & 2 & \dots & n-1 \end{vmatrix} = (-1)^{n+2}\cdot \begin{vmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 2 \\ \dots & \dots & \dots & \dots \\ 1 & 2 & \dots & n-1 \end{vmatrix}$$

By induction, we get that

$$\Delta = (-1)^{(n+2)+(n+1)+\dots+2} \cdot \begin{vmatrix} 1 & 1 \\ 1 & 2 \end{vmatrix} = (-1)^{\frac{(n+1)(n+4)}{2}} \neq 0$$

So, they form a basis in $\mathbb{R}^n$.

For a vector $(x_1, x_2, \dots, x_n) = \alpha_1 v_1 + \dots \alpha_n v_n$

$$\begin{cases} \alpha_1 + \alpha_2 + \dots + \alpha_{n-1} + \alpha_n = x_1 \\ \alpha_1 + \alpha_2 + \dots + \alpha_{n-1} + 2\alpha_n = x_2 \\ \alpha_1 + \alpha_2 + \dots + 2\alpha_{n-1} + 3\alpha_n = x_3 \\ \vdots \end{cases}$$

If we compute $L_2 - L_1$ we get that $\alpha_n = x_2 - x_1$. Then $L_3 - L_2$, we get $\alpha_{n-1} = x_3 - 2x_2 + x_1$. So on, by induction, we get that:

$$\begin{cases} \alpha_{n-p} = x_{p+2} - 2x_{p+1} + x_p, \text{ if } p \geq 1 \\ \alpha_n = x_2 - x_1, \text{ if } p = 0 \end{cases}$$

7. We know that (E_1, E_2, E_3, E_4) is a basis in $M_2(\mathbb{R})$ and so, the coordinates of B in the basis are $(2, 1, 1, 0)$.

   For the second one we have to solve the system $a_1A_1 + a_2A_2 + a_3A_3 + a_4A_4 = 0 \Rightarrow a_1 = a_2 = a_3 = a_4 = 0 \Rightarrow A_1, A_2, A_3, A_4$ are linearly independent. Then $\forall A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{R}), \exists! a_1, a_2, a_3, a_4 \in \mathbb{R}$ such that $a_1A_1 + a_2A_2 + a_3A_3 + a_4A_4 = A \Rightarrow \begin{cases} a_1 = a - b \\ a_2 = b - c \\ a_3 = c - d \\ a_4 = d \end{cases}$

   $\Rightarrow < A_1, A_2, A_3, A_4 >= M_2(\mathbb{R})$ so it is a basis of $M_2(\mathbb{R})$. Then, the coordinates of B is this basis are $(1, 0, 1, 0)$.

8. We know that E is a basis in $\mathbb{R}_2[X]$ and so, the coordinates of f in E are (a_0, a_1, a_2).

   For the second one, we have

   $$\alpha_1 \cdot 1 + \alpha_2 \cdot (X - a) + \alpha_3 \cdot (X - a^2) = 0 \iff \begin{cases} \alpha_1 - a\alpha_2 + a^2\alpha_3 = 0 \\ \alpha_2 - 2\alpha_3 = 0 \\ \alpha_3 = 0 \end{cases}$$

   $\Rightarrow \alpha_1 = \alpha_2 = \alpha_3 = 0 \Rightarrow B$ has linearly independent vectors.

   $\forall f = b_0 + b_1X + b_2X^2 \in \mathbb{R}_2[X], \exists! \alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$ such that

   $$f = \alpha_1 \cdot 1 + \alpha_2 \cdot (X - a) + \alpha_3 \cdot (X - a^2) \Rightarrow \begin{cases} \alpha_1 = b_0 + ab_1 - a^2b_2 \\ \alpha_2 = b_1 + 2ab_2 \\ \alpha_3 = b_2 \end{cases}$$

   $\Rightarrow < B >= \mathbb{R}_2[X] \Rightarrow B$ is a basis of $\mathbb{R}_2[X]$. And so, the coordinates of B in this basis are $(a_0 + aa_1 - a^2a_2, a_1 + 2aa_2, a_2)$.

9. $\mathbb{Z}_2^3 = \{(\hat{0}, \hat{0}, \hat{0}), (\hat{1}, \hat{0}, \hat{0}), (\hat{0}, \hat{1}, \hat{0}), (\hat{0}, \hat{0}, \hat{1}), (\hat{1}, \hat{1}, \hat{0}), (\hat{1}, \hat{0}, \hat{1}), (\hat{0}, \hat{1}, \hat{1}), (\hat{1}, \hat{1}, \hat{1})\}$.

   So, $\mid \mathbb{Z}_2^3 \mid= 2^3$.

   A pair $(z_1, z_2, z_3) \in \mathbb{Z}_2^3$ is a base $\iff$ z_1, z_2, z_3 are linearly independent.

   Take $z_1 \in \mathbb{Z}_2^3 \setminus \{(\hat{0}, \hat{0}, \hat{0})\} \Rightarrow z_1$ is a part of the base $\Rightarrow z_1$ can be chosen in $2^3 - 1$ ways. If $z_2, z_3 \in \mathbb{Z}_2^3 \Rightarrow z_1, z_2, z_3$ linearly independent $\iff z_2 \in \mathbb{Z}_2^3 \setminus < z_1 >$ and $z_3 \in \mathbb{Z}_2^3 \setminus < z_1, z_2 >$. So, z_2 can be chosen in

$(2^3-1)-1$ ways and z_3 in $((2^3-2)-1)-1$ ways. Hence, the number of basis of $\mathbb{Z}_2^3$ is $(2^3-1)(2^3-2)(2^3-4)=168$.

10. It is the same thing as finding how many basis are in $\mathbb{Z}_2^3$.

Seminar 7

The dimension of a space is given by the number of vectors in its (canonical) basis.

If $f : V \to V$, then $dim(V) = dim(ker(f)) + dim(Im(f))$.

If $ker(f) = \{0\}$, then $dim(ker(f)) = 0$.

If $A \subseteq B$, then $dim(A) \leq dim(B)$.

We have: $dim(A) + dim(B) = dim(A + B) + dim(A \cap B)$.

$\bar{S}$ is a complement of S, where $S \bigoplus \bar{S} = V$, the whole space.

1. $A = \{(x, y, z) \in \mathbb{R}^3 \mid z = 0\} = \{(x, y, 0) \mid x, y \in \mathbb{R}\} = \{(x, 0, 0) + (0, y, 0) \mid x, y \in \mathbb{R}\} = \{x(1, 0, 0)+y(0, 1, 0) \mid x, y \in \mathbb{R}\} =< (1, 0, 0), (0, 1, 0) >$ which is a basis if the vectors are linearly independent $\iff a(1, 0, 0)+ b(0, 1, 0) = (0, 0, 0) \iff (a, b, 0) = (0, 0, 0) \Rightarrow a = b = 0$ (true) $\Rightarrow< (1, 0, 0), (0, 1, 0) >$ is a base of A. So, $dim(A) = 2$.

   $B = \{(x, y, z) \in \mathbb{R}^3 \mid x + y + z = 0\} = \{(x, y, z) \in \mathbb{R}^3 \mid z = -x - y\} = \{(x, y, -x - y) \mid x, y \in \mathbb{R}\} = \{(x, 0, -x) + (0, y, -y) \mid x, y \in \mathbb{R}\} = \dots =< (1, 0, -1), (0, 1, -1) >$ which is a basis if the vectors are linearly independent $\iff a(1, 0, -1) + b(0, 1, -1) = (0, 0, 0) \Rightarrow a = b = 0 \Rightarrow$ is a base of B. So, $dim(B) = 2$.

   $C = \{(x, y, z) \in \mathbb{R}^3 \mid x = y = z\} = \{(x, x, x) \mid x \in \mathbb{R}\} = \dots =$ $< (1, 1, 1) >$ which is a basis, as we have one vector (so linearly independent). So, $dim(C) = 1$.

2. (i) S is a subspace of K^n if $S \neq \emptyset$ (which is true, as $(0, 0, \dots, 0) \in S$) and $\forall a, b \in K, \forall x, y \in S \Rightarrow ax + by \in S$. So, $ax + by = a(x_1, \dots, x_n) + b(y_1, \dots, y_n) = \dots = (ax_1 + by_1, \dots, ax_n + by_n)$, which is in S if $ax_1 + by_1 + \dots + ax_n + by_n = 0 \iff a(x_1 + \dots x_n) + b(y_1 + \dots y_n) = a \cdot 0 + b \cdot 0 = 0 \Rightarrow S$ is a subspace of K^n.

   (ii) From $x_1 + \dots + x_n = 0 \Rightarrow x_n = -x_1 - x_2 \dots - x_{n-1}$.
   So, $S = \{(x_1, \dots, x_{n-1}, -x_1 - \dots - x_{n-1}) \mid x_1, \dots, x_{n-1} \in K\} = \{(x_1, 0, \dots, 0, -x_1)+\dots+(0, 0, \dots, 0, x_{n-1}, -x_{n-1}) \mid x_1, \dots, x_{n-1} \in K\} = \dots =< (1, 0, \dots, 0, -1), \dots, (0, 0, \dots, 0, 1, -1) >$ which is a basis if the vectors are linearly independent (you can prove this yourselves). So, $dim(S) = n - 1$.

3. We know that $(\mathbb{C}, +)$ is an Abelian group. Now, for $\mathbb{C}$ to be a vector space, we need to see if the 4 conditions hold:

(a) $(k_1 + k_2)z = k_1 z + k_2 z$ (true)
(b) $k(z_1 + z_2) = kz_1 + kz_2$ (true)
(c) $(k_1 k_2)z = k_1(k_2 z)$ (true)
(d) $1 \cdot z = z$ (true)

Now, $\forall z \in \mathbb{C}, \exists a, b \in \mathbb{R}$ such that $z = a \cdot 1 + b \cdot i \Rightarrow \mathbb{C} =< 1, i >$ which is a basis, as 1 and i are linearly independent and $dim(\mathbb{C}) = 2$.

4. f is an $\mathbb{R}$-linear map if $\forall a, b \in \mathbb{R}, \forall x, y \in \mathbb{R}^3 : f(ax + by) = af(x) + bf(y)$.

   So, $f(a(x_1, x_2, x_3) + b(y_1, y_2, y_3)) = f(ax_1 + by_1, ax_2 + by_2, ax_3 + by_3) = \cdots = a(x_2, -x_1) + b(y_2, -y_1) = af(x) + bf(y)$.

   $ker(f) = \{(x, y, z) \in \mathbb{R}^3 \mid f(x, y, z) = (0, 0)\} = \{(x, y, z) \in \mathbb{R}^3 \mid (y, -x) = (0, 0)\} = \{(0, 0, z) \mid z \in \mathbb{R}\} =< (0, 0, 1) >$.

   So, $dim(ker(f)) = 1$.

   $Im(f) = \{(y, -x) \in \mathbb{R}^2 \mid f(x, y, z) = (y, -x)\} = \{(y, 0) + (0, -x) \mid x, y \in \mathbb{R}\} =< (1, 0), (0, -1) >$. So, $dim(Im(f)) = 2$.

5. $ker(f) = \{(x, y, z) \in \mathbb{R}^3 \mid (-y+5z, x, y-5z) = (0, 0, 0)\} \Rightarrow -y+5z = 0$ and $x = 0$ and $y - 5z = 0 \Rightarrow x = 0$ and $y = 5z \Rightarrow ker(f) = \{(0, 5z, z) \mid z \in \mathbb{R}\} =< (0, 5, 1) >$, with $dim(ker(f)) = 1$.

   $Im(f) = \{(-y+5z, x, y-5z) \in \mathbb{R}^3 \mid f(x, y, z) = (-y, 0, y) + (5z, 0, -5z) + (0, x, 0)\} =< (-1, 0, 1), (5, 0, -5), (0, 1, 0) >$, but $(5, 0, -5) = -5(-1, 0, 1)$ (i.e. they are not linearly independent) so a basis for $Im(f) =< (-1, 0, 1), (0, 1, 0) >$, with $dim(Im(f)) = 2$.

6. For A we need to find a third vector in the basis, which is linearly independent with the other two. So, $a(1, 0, 0) + b(0, 1, 0) + c(x, y, z) = (0, 0, 0) \iff a = b = c = 0 \Rightarrow a + cx = 0$ and $b + cy = 0$ and $cz = 0 \Rightarrow x, y, z \in \mathbb{R}$ (not all zero) $\Rightarrow (x, y, z) = (0, 0, 1)$.

   For B the same as above $\Rightarrow a(1, 0, -1) + b(0, 1, -1) + c(x, y, z) = (0, 0, 0) \iff a = b = c = 0 \Rightarrow a + cx = 0$ and $b + cy = 0$ and $-a-b+cz = 0 \Rightarrow c(x+y+z) = 0 \Rightarrow x+y+z \neq 0 \Rightarrow (x, y, z) = (1, 1, 0)$.

   For C we need to find two vectors in the basis, which are linearly independent with the third one. So, we can add the vectors $(a, b, c) = (1, 1, 0)$ and $(x, y, z) = (1, 0, 1)$.

7. (i) We can easily see that $A =< (-2,1,0), (-3,0,1) >$. So, we need to complete this generator to a basis in $\mathbb{R}^3$.

   Let (a,b,c) be the vector we need to put there:

   $\Rightarrow \begin{vmatrix} -2 & 1 & 0 \\ -3 & 0 & 1 \\ a & b & c \end{vmatrix} \neq 0 \Rightarrow a + 2b + 3c \neq 0.$

   So, we can take $a = 0, b + 0, c + 1 \Rightarrow (0,0,1)$ generates the complement of A.

   $\bar{A} =< (0,0,1) >= \{(0,0,z) \mid z \in \mathbb{R}\}$.

   (ii) $B =< (1,0,0), (0,0,1) >$ so, to complete it to $\mathbb{R}_3[X]$ we need to add another vector. It is easy to see that we can take a vector from the canonical basis $(0,1,0)$. So, $\bar{B} =< (0,1,0) >= \{cX^2 \mid c \in \mathbb{R}\}$.

8. $dim(S) + dim(U) = dim(S \cap U) + dim(S+U) = dim(T \cap U) + dim(T + U) = dim(T) + dim(U) \Rightarrow dim(S) = dim(T)$. As $S \subseteq T$, we know $dim(S) \leq dim(T)$. So, if their dimensions are equal $\Rightarrow S = T$.

9. First, rewrite S as a generated subset and T as a set.

   $S =< (0,1,0), (0,0,1) >$ and $T = \{(x,y,z) \in \mathbb{R}^3 \mid x - y + z = 0\}$ (you can simply find those).

   Now, $S \cap T = \{(x,y,z) \in \mathbb{R}^3 \mid x = 0$ and $x - y + z = 0\} = \{(x,y,z) \in \mathbb{R}^3 \mid x = 0$ and $y = z\} =< (0,1,1) >$, with $dim(S \cap T) = 1$.

   As, $S, T \subseteq \mathbb{R}^3 \Rightarrow S + T \subseteq \mathbb{R}^3 \Rightarrow dim(S+T) \leq dim(\mathbb{R}^3) = 3$.

   From $dim(S) + dim(T) = dim(S \cap T) + dim(S+T)$ and $dim(S) = dim(T) = 2 \Rightarrow 2 + 2 = 1 + dim(S+T) \Rightarrow dim(S+T) = 4 - 1 = 3 = dim(\mathbb{R}^3) \Rightarrow S + T = \mathbb{R}^3$.

10. For S we need to see if the vetors are linearly independent.

    $a \cdot \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + b \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

    We obtain the system: $\begin{cases} a + b = 0 \\ a = 0 \\ b = 0 \end{cases} \Rightarrow$ they are linearly independent, so $dim(S) = 2$.

    The same goes for $T \Rightarrow a \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} b \cdot \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

We obtain the system: $\begin{cases} a = 0 \\ a + b = 0 \\ b + 0 \end{cases}$ $\Rightarrow$ they are linearly independent, so $dim(T) = 2$.

We know that $dim(S+T) = dim(S \cup T)$, so we need to see how many vectors (from both generators) are linearly independent.

$a \cdot \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + b \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} + c \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} d \cdot \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

We obtain the system: $\begin{cases} a + b = 0 \Rightarrow a = -b \\ a + c = 0 \Rightarrow c = -a \Rightarrow c = b \\ b + c + d = 0 \Rightarrow b + b - b = 0 \Rightarrow b = 0 \\ b + d = 0 \Rightarrow d = -b \end{cases}$

$\Rightarrow a = b = c = d = 0 \Rightarrow$ they are all linearly independent. So, $dim(S+T) = 4$.

Since $dim(S) + dim(T) = dim(S+T) + dim(S \cap T) \Rightarrow dim(S \cap T) = 0$.

Seminar 8

A matrix A is **invertible** if $det(A) \neq 0$.

Kronecker-Capelli: a system is compatible if $Rang(A) = Rang(\bar{A})$, where A is the matrix of the system and $\bar{A}$ is A with a column consisting of the free terms.

Rouche: a system is compatible if all the characteristic determinants are zero.

Cramer: $x_i = \frac{det(A_i)}{det(A)}$ are the solutions of a system, where A_i is the matrix A, by replacing the column i with the column of the free terms.

Gauss-Jordan: zeros under the main diagonal.

1. The matrix A is invertible if $det(A) \neq 0 \iff det(A) = -1 \neq 0$.

   $A^{-1} = \frac{1}{det(A)} A^* \iff A^{-1} = \begin{bmatrix} 3 & -4 & 2 \\ -5 & 7 & -3 \\ 9 & -12 & 5 \end{bmatrix}$.

   $AX = B \mid A^{-1} \cdot \Rightarrow X = A^{-1}B \Rightarrow \begin{cases} x_1 = 7 \\ x_2 = -11 \\ x_3 = 19 \end{cases}$.

2. (i) $\bar{A} = \begin{bmatrix} 1 & 1 & 1 & -2 & | & 5 \\ 2 & 1 & -2 & 1 & | & 1 \\ 2 & -3 & 1 & 2 & | & 3 \end{bmatrix}$. So $Rang(A) = Rang(\bar{A}) = 3 \Rightarrow$ compatible system with "number of columns - $Rang(A)$" unknowns, i.e. 1 unknown. Let's say $x_4 = \alpha \in \mathbb{R}$, then the system becomes:

   $$\begin{cases} x_1 = 5 - x_2 - x_3 + 2\alpha \\ 10 - 2x_2 - 2x_3 + 4\alpha + x_2 - 2x_3 + \alpha = 1 \\ 10 - 2x_2 - 2x_3 + 4\alpha - 3x_2 + x_3 + 2\alpha = 3 \end{cases}$$

   By solving the system, we get that $x_1 = 2$, $x_2 = 1 + \alpha$, $x_3 = 2 + \alpha$ and $x_4 = \alpha$, with $\alpha \in \mathbb{R}$.

   (ii) $\bar{A} = \begin{bmatrix} 1 & -2 & 1 & 1 & | & 1 \\ 1 & -2 & 1 & -1 & | & -1 \\ 1 & -2 & 1 & 5 & | & 5 \end{bmatrix}$. So $Rang(A) = Rang(\bar{A}) = 2$, by using the submatrix $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \Rightarrow$ compatible system with 2 unknowns. Let's take $x_1 = \alpha$ and $x_2 = \beta$ both in $\mathbb{R}$, then the system becomes:

$$\begin{cases} x_3 + x_4 = 1 - \alpha + 2\beta \\ x_3 - x_4 = -1 - \alpha + 2\beta \\ x_3 + 5x_4 = 5 - \alpha + 2\beta \end{cases}$$

By solving the system, we get that $x_1 = \alpha$, $x_2 = \beta$, $x_3 = -\alpha + 2\beta$ and $x_4 = 1$, with $\alpha, \beta \in \mathbb{R}$.

(iii) $\bar{A} = \begin{bmatrix} 1 & 1 & 1 & | & 3 \\ 1 & -1 & 1 & | & 1 \\ 2 & -1 & 2 & | & 3 \\ 1 & 0 & 1 & | & 4 \end{bmatrix}$. So, $Rang(A) = 2 \neq 3 = Rang(\bar{A}) \Rightarrow$ incompatible system.

3. Similar to the previous exercise.

4. $A = \begin{bmatrix} b & a & 0 \\ c & 0 & a \\ 0 & c & b \end{bmatrix} \Rightarrow det(A) = -2abc$. Then the system is compatible determinate if $det(A) \neq 0 \iff abc \neq 0 \iff a, b, c \neq 0$.

Now, let's compute the solutions: $x = \frac{det(A_x)}{det(A)}$, where $det(A_x) = \begin{vmatrix} c & a & 0 \\ b & 0 & a \\ a & c & b \end{vmatrix} \Rightarrow$

$$\begin{cases} x = \frac{b^2+c^2-a^2}{2bc} \\ y = \frac{a^2+c^2-b^2}{2ac} \\ z = \frac{b^2+a^2-c^2}{2ab} \end{cases}$$

5. (i) $\begin{bmatrix} 2 & 2 & 3 & | & 3 \\ 1 & -1 & 0 & | & 1 \\ -1 & 2 & 1 & | & 2 \end{bmatrix}$. We change L_2 with $L_1 \Rightarrow \begin{bmatrix} 1 & -1 & 0 & | & 1 \\ 2 & 2 & 3 & | & 3 \\ -1 & 2 & 1 & | & 2 \end{bmatrix}$.

We do $L_2 = L_2 - 2L_1$ and $L_3 = L_3 + L_1 \Rightarrow \begin{bmatrix} 1 & -1 & 0 & | & 1 \\ 0 & 4 & 3 & | & 1 \\ 0 & 1 & 1 & | & 3 \end{bmatrix}$.

Again $L_1 = L_1 + L_3$ and $L_2 = L_2 - 3L_3 \Rightarrow \begin{bmatrix} 1 & 0 & 1 & | & 4 \\ 0 & 1 & 0 & | & -8 \\ 0 & 1 & 1 & | & 3 \end{bmatrix}$.

Then $L_3 = L_3 - L_2 \Rightarrow \begin{bmatrix} 1 & 0 & 1 & | & 4 \\ 0 & 1 & 0 & | & -8 \\ 0 & 0 & 1 & | & 11 \end{bmatrix}$. In the end $L_1 = L_1 - L_3 \Rightarrow \begin{bmatrix} 1 & 0 & 0 & | & -7 \\ 0 & 1 & 0 & | & -8 \\ 0 & 0 & 1 & | & 11 \end{bmatrix} \Rightarrow \begin{cases} x = -7 \\ y = -8 \\ z = 11 \end{cases}$.

(ii) I shall write only the operations on lines, so: $\begin{cases} L_3 \leftrightarrow L_1 \\ L_2 = L_2 - L_1, L_3 = L_3 - 2L_1 \\ L_3 = L_3 - 3L_2 \\ L_1 = L_1 - L_2 \end{cases} \Rightarrow$

$\begin{bmatrix} 1 & 0 & -7 & | & 1 \\ 0 & 1 & 3 & | & 1 \\ 0 & 0 & 0 & | & 0 \end{bmatrix}$. As the last line is all zeros, then the third unknown is $z = \alpha \in \mathbb{R} \Rightarrow x = 1 + 7\alpha$ and $y = 1 - 3\alpha$.

(iii) I shall write only the operations on lines, so: $\begin{cases} L_2 = L_2 - L_1, L_3 = L_3 - 2L_1, L_4 = L_4 - L_1 \\ L_2 = L_2 - 2L_4, L_3 = L_3 - 3L_4 \end{cases}$

$\begin{bmatrix} 1 & 1 & 1 & | & 3 \\ 0 & 0 & 0 & | & -4 \\ 0 & 0 & 0 & | & -6 \\ 0 & -1 & 0 & | & 1 \end{bmatrix} \Rightarrow \begin{cases} x + y + z = 3 \\ -y = 1 \end{cases} \Rightarrow y = -1,\ z = \alpha \in \mathbb{R}$ and $x = 4 - \alpha$.

6. I shall write only the operations on lines, so: $\begin{cases} L_2 \leftrightarrow L_1 \\ L_2 = L_2 - 2L_1, L_3 = L_3 - L_1 \\ L_3 = L_3 + L_2 \end{cases} \Rightarrow$

$\begin{bmatrix} 1 & 2 & -1 & 4 & | & 2 \\ 0 & -3 & 3 & -7 & | & -3 \\ 0 & 0 & 0 & 0 & | & \lambda - 2 - 3 \end{bmatrix} \Rightarrow \begin{cases} x_1 + 2x_2 - x_3 + 4x_4 = 2 \\ -3x_2 + 3x_3 - 7x_4 = -3 \\ 0 = \lambda - 2 - 3 \\ x_1 = \alpha \\ x_4 = \beta \end{cases}$. By solving this system we get that $\lambda = 5$, $x_2 = 1 - \alpha - \frac{5}{3}\beta$ and $x_3 = -\alpha + \frac{2}{3}\beta$.

7. I shall write only the operations on lines, so: $\begin{cases} L_3 \leftrightarrow L_1 \\ L_2 = L_2 - L_1 \\ L_3 = L_3 - aL_1 \\ L_3 = L_3 + L_2 \end{cases} \Rightarrow$

$$\begin{bmatrix} 1 & 1 & a & | & a^2 \\ 0 & a-1 & 1-a & | & a-a^2 \\ 0 & 0 & 2-a-a^2 & | & 1-a^3+a-a^2 \end{bmatrix} \Rightarrow \begin{cases} x+y+az = a^2 \\ (a-1)y+(1-a)z = a(1-a) \\ (2-a-a^2)z = 1-a^2+a-a^3 \end{cases} .$$

By solving the system we get: $\begin{cases} x = -1-a \\ y = 1 \\ z = 1+a \end{cases}$

8. We have two ways to solve it.

(a) $\begin{cases} xyz = 1 \\ x^3y^2z^2 = 27 \\ \frac{z}{xy} = 81 \end{cases} \Rightarrow \begin{cases} z = \frac{1}{xy} \\ z^2 = \frac{27}{x} \cdot \frac{1}{x^2y^2} \\ z = 81xy \end{cases} \Rightarrow \frac{27}{x} = 1 \Rightarrow x = 3^3.$

Now, $\frac{1}{xy} = 81xy \iff \frac{1}{3^3y} = 3^4 \cdot 3^3y \iff y^2 = \frac{1}{3^{10}}$, with $0 \leq y \Rightarrow y = \frac{1}{3^5}$. And $z = 81 \cdot 3^3 \cdot \frac{1}{3^5} \Rightarrow z = 3^2$.

(b) What if we apply log_3 for each equation?!

We will get: $\begin{cases} log_3(x+y+z) = log_3(3^0) \\ log_3(x^3y^2z^2) = log_3(3^3) \\ log_3(\frac{z}{xy}) = log_3(3^4) \end{cases} .$

And from here, we get to the same solution. (Try this at home!)

Seminar 9

1. We have the matrix $\begin{bmatrix} 0 & 2 & 3 \\ 2 & 4 & 3 \\ 1 & 1 & 1 \\ 2 & 2 & 4 \end{bmatrix}$.

   I shall write only the operations on lines: $\begin{cases} L3 \leftrightarrow L1 \\ L2 = L2 - 2L1, L4 = L4 - 2L1 \\ L3 = L3 - L2, L4 = L4 - L3 \end{cases}$

   We get to the matrix: $\begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{bmatrix}$.We have one line of zeros, so the rank comes from the other three $\Rightarrow Rank = 3$.

2. Now we have the matrix $\begin{bmatrix} 1 & -1 & 3 & 2 \\ -2 & 0 & 3 & -1 \\ -1 & 2 & 0 & -1 \end{bmatrix}$.

   I shall write only the operations on lines: $\begin{cases} L2 = L2 + 2L1, L3 = L3 + L1 \\ L3 = 2L3 + L2 \\ L2 = \frac{1}{2}(L2 + L3) \\ L1 = L1 - L3 \end{cases}$

   We get the matrix: $\begin{bmatrix} 1 & 0 & 0 & -3 \\ 0 & -1 & 0 & 4 \\ 0 & 0 & 3 & 5 \end{bmatrix}$. We see the first three columns that get our non-zero determinant, so the rank is 3.

3. The same as *Exercise 2*.

4. For this, we put near our matrix, the identity matrix.

   $\begin{bmatrix} 1 & 2 & 2 & | & 1 & 0 & 0 \\ 2 & 1 & -2 & | & 0 & 1 & 0 \\ 2 & -2 & 1 & | & 0 & 0 & 1 \end{bmatrix}$.

   Now, $L2 = L2 - 2L1$ and $L3 = L3 - 2L1$: $\begin{bmatrix} 1 & 2 & 2 & | & 1 & 0 & 0 \\ 0 & -3 & -6 & | & -2 & 1 & 0 \\ 0 & -6 & -3 & | & -2 & 0 & 1 \end{bmatrix}$.

From here $L3 = L3 - 2L2$ and $\begin{bmatrix} 1 & 2 & 2 & | & 1 & 0 & 0 \\ 0 & -3 & -6 & | & -2 & 1 & 0 \\ 0 & 0 & 9 & | & 2 & -2 & 1 \end{bmatrix}$.

Then $L1 = 3L1 + 2L2$, so $\begin{bmatrix} 3 & 0 & 6 & | & -1 & 2 & 0 \\ 0 & -3 & -6 & | & -2 & 1 & 0 \\ 0 & 0 & 9 & | & 2 & -2 & 1 \end{bmatrix}$.

It is obvious that we can do $L1 = \frac{1}{3}L1$, $L2 = -\frac{1}{3}L2$ and $L3 = \frac{1}{9}L3$.
$\begin{bmatrix} 1 & 0 & -2 & | & -\frac{1}{3} & \frac{2}{3} & 0 \\ 0 & 1 & 2 & | & \frac{2}{3} & -\frac{1}{3} & 0 \\ 0 & 0 & 1 & | & \frac{2}{9} & -\frac{2}{9} & \frac{1}{9} \end{bmatrix}$.

In the end, $L2 = L2 - 2L3$ and $L1 = L1 + 2L3$: $\begin{bmatrix} 1 & 0 & 0 & | & -\frac{1}{9} & \frac{2}{9} & \frac{2}{9} \\ 0 & 1 & 0 & | & \frac{2}{9} & \frac{1}{9} & -\frac{2}{9} \\ 0 & 0 & 1 & | & \frac{2}{9} & -\frac{2}{9} & \frac{1}{9} \end{bmatrix}$.

So, we get on the first part the identity matrix and on the second part the inverse of our initial matrix.

5. The same as *Exercise 4*.

6. We build the matrix $X = \begin{bmatrix} 3 & 2 & -5 & 4 \\ 3 & -1 & 3 & -3 \\ 3 & 5 & -13 & 11 \end{bmatrix}$.

   By applying $L_2 - L_1$, $L_3 - L_1$ and then $L_3 + L_2$, we obtain the echelon form $X = \begin{bmatrix} 3 & 2 & -5 & 4 \\ 0 & -3 & 8 & -7 \\ 0 & 0 & 0 & 0 \end{bmatrix}$.

   As, the last raw is formed only of zeroes, the three vectors $v_!, v_2, v_3$ are linearly dependent.

7. We build the matrix $\begin{bmatrix} 1 & 0 & 4 \\ 2 & 1 & 0 \\ 1 & 5 & -36 \\ 2 & 10 & -72 \end{bmatrix}$.

   I shall write only the operations on lines: $\begin{cases} L4 = L4 - 2L3 \\ L2 = L2 - 2L1, L3 = L3 - L1 \\ L3 = \frac{1}{5}L3 \\ L3 = L3 - L2 \end{cases}$

We obtain the matrix: $\begin{bmatrix} 1 & 0 & 4 \\ 0 & 1 & -8 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$.

So the rank is $2 \Rightarrow dim < X >= 2 \Rightarrow < X >=< v1, v2 >$ (given by the vectors forming the non-zero lines).

8. The same as *Exercise 7*.

9. For S we have the matrix $\begin{bmatrix} 1 & 0 & 4 \\ 2 & 1 & 0 \\ 1 & 1 & -4 \end{bmatrix}$. If we do $L3+L3+L1$ and after that $L3 = L3 - L2$ we get to the matrix $\begin{bmatrix} 1 & 0 & 4 \\ 2 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$. So, $dim(S) = 2$ and $S =< (1, 0, 4), (2, 1, 0) >$.

For T we have the matrix $\begin{bmatrix} -3 & -2 & 4 \\ 5 & 2 & 4 \\ -2 & 0 & -8 \end{bmatrix}$. If we do $L2 = L2 + L1$ and after that $L3 = L3 + L2$ we get to the matrix $\begin{bmatrix} -3 & -2 & 4 \\ 2 & 0 & 8 \\ 0 & 0 & 0 \end{bmatrix}$.

So $dim(T) = 2$ and $T =< (-3, -2, 4), (5, 2, 4) >$.

Remember: $dim(S+T) = dim < S \cup T >$ and $dim(S+T) = dim(S) + dim(T) - dim(S \cap T)$.

For $S + T$ we have the matrix $\begin{bmatrix} 1 & 0 & 4 \\ 2 & 1 & 0 \\ 1 & 1 & -4 \\ -3 & -2 & 4 \\ 5 & 2 & 4 \\ -2 & 0 & -8 \end{bmatrix}$.

The operations on lines are: $\begin{cases} L3 = L3 + L1, L5 = L5 + L4 \\ L3 = L3 - L2, L6 = L6 + L5 \\ L5 = L5 - 2L1 \end{cases}$.

And we get to the matrix $\begin{bmatrix} 1 & 0 & 4 \\ 2 & 1 & 0 \\ 0 & 0 & 0 \\ -3 & -2 & 4 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$. So, $dim(S+T) = 3$ and $< S+T > = < (1,0,4),(2,1,0),(-3,-2,4) >$.

So, the dimension for $S \cap T$ is obtained from the equality above, hence $dim(S \cap T) = 1$.

10. The same as *Exercise 9*.

Seminar 10

$[f]_E = [f(e_1) \mid f(e_2) \mid f(e_3)]$.

If we have the bases $B = e \cdot S$ and $B' = e' \cdot T$, then $[f]_{BB'} = T^{-1} \cdot [f]_{ee'} \cdot S$.

$[f]_E \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$ for a basis in $ker(f)$.

$dim(Im(f)) = dim(f(e)) = dim(< f(e_1), f(e_2), f(e_3), f(e_4) >) =$ maximum number of linearly independent vectors in $[f]_E = rank([f]_E)$.

f is an automorphism $\iff det([f]_E) \neq 0$ and $[2f]_E = 2[f]_E$.

1. We use $[f]_E = [f(e_1)f(e_2)f(e_3)]$. So, we compute $\begin{cases} f(e_1) = f(1,0,0) = (1,0,2) \\ f(e_2) = f(0,1,0) = (1,1,1) \\ f(e_3) = f(0,0,1) = (0,-1,1) \end{cases}$

   Hence, $[f]_E = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & -1 \\ 2 & 1 & 1 \end{bmatrix}$.

2. $\begin{cases} f(v_1) = f(1,1,0) = (1,-1) \\ f(v_2) = f(0,1,1) = (1,0) \\ f(v_3) = f(1,0,1) = (0,-1) \end{cases}$

   So, $[f]_{BE'} = \begin{bmatrix} 1 & 1 & 0 \\ -1 & 0 & -1 \end{bmatrix}$.

   From $f(v_1) = (1,-1)$, we get $(1,-1) = a_1v_1' + a_2v_2' = (a_1 + a_2, a_1 - 2a_2) \Rightarrow a_2 = \frac{2}{3}$ and $a_1 = \frac{1}{3}$.

   From $f(v_2) = (1,0)$, we get $(1,0) = a_1v_1' + a_2v_2' = (a_1 + a_2, a_1 - 2a_2) \Rightarrow a_2 = \frac{1}{3}$ and $a_1 = \frac{2}{3}$.

   From $f(v_3) = (0,-1)$, we get $(0,-1) = a_1v_1' + a_2v_2' = (a_1 + a_2, a_1 - 2a_2) \Rightarrow a_2 = \frac{1}{3}$ and $a_1 = -\frac{1}{3}$.

   Hence, $[f]_{BB'} = \begin{bmatrix} \frac{1}{3} & \frac{2}{3} & -\frac{1}{3} \\ \frac{2}{3} & \frac{1}{3} & \frac{1}{3} \end{bmatrix}$.

3. (i) Let $v = (a,b,c) \in \mathbb{R}^3 \Rightarrow f(v) = f(ae_1 + be_2 + ce_3) \iff f(v) = af(e_1) + bf(e_2) + cf(e_3)$, as f is an homomorphism.

   Hence, $f(v) = a + 4b - 2c, 2a + 3b + c, 3a + 2b + 4c, 4a + b + c) \in \mathbb{R}^4$

(ii) $[f]_E = \begin{bmatrix} 1 & 4 & -2 \\ 2 & 3 & 1 \\ 3 & 2 & 4 \\ 4 & 1 & 1 \end{bmatrix}$

(iii) $[f]_e \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \iff \begin{cases} x_1 + 4x_2 - 2x_3 = 0 \\ 2x_1 + 3x_2 + x_3 = 0 \\ 3x_1 + 2x_2 + 4x_3 = 0 \\ 4x_1 + x_2 + x_3 = 0 \end{cases}$

$$\bar{A} = \begin{bmatrix} 1 & 4 & -2 & \mid & 0 \\ 2 & 3 & 1 & \mid & 0 \\ 3 & 2 & 4 & \mid & 0 \\ 4 & 1 & 1 & \mid & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 4 & -2 & \mid & 0 \\ 0 & -1 & 1 & \mid & 0 \\ 0 & 0 & 0 & \mid & 0 \\ 0 & 0 & 0 & \mid & 0 \end{bmatrix} \Rightarrow \begin{cases} x_3 = \alpha \in \mathbb{R} \\ x_2 = \alpha \\ x_1 = -2\alpha \end{cases} \Rightarrow$$

$ker(f) =< (-2, 1, 1) >\Rightarrow dim(ker(f)) = 1.$

For the image, we have the matrix: $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ -2 & 1 & 4 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & -1 & -1 & -5 \\ 0 & 0 & 0 & -6 \end{bmatrix} \Rightarrow$

$dim(Im(f)) = 3.$

4. (i) $v = (1, 4, 1, -1) = e_1 + 4e_2 + e_3 - e_4 \Rightarrow f(v) = f(e_1) + 4f(e_2) + f(e_3) - f(e_4) = (1, -1, 2, 1) + 4(1, 1, 1, 2) + (-3, 1, -5, -4) - (2, 4, 1, 5) = (0, 0, 0, 0) \Rightarrow v \in ker(f).$

$v' \in Im(f) \iff \exists v$ such that $f(v) = v'$. So, $v' = af(e_1) + bf(e_2) + cf(e_3) + df(e_4) \Rightarrow \begin{cases} a + b - 3c + 2d = 2 \\ -a + b + c + 4d = -2 \\ 2a + b - 5c + d = 4 \\ a + 2b - 4c + 5d = 2 \end{cases}$.

By solving the system, we get that $c, d \in \mathbb{R}$, $b = c - 3d$ and $a = 2 + 2c + d$. Hence, there is a v such that $f(v) = v'$.

(ii) We use $[f]_E \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$. By solving the system here, we get that $x_4 = a$, $x_3 = b$, $x_2 = b - 3a$ and $x_1 = 2b + a \iff < (1, -3, 0, 1), (2, 1, 1, 0) >= ker(f) \Rightarrow dim = 2.$

We use $dim(Im(f)) = rank[f]_E$ and we know that $rank[f]_E = 2 \Rightarrow dim(Im(f)) = 2$ and $Im(f) =< (1, 1, -3, 2), (-1, 1, 1, 4) >.$

(iii) $\begin{cases} f(1,0,0,0) = (1,-1,2,1) = (x,-x,2x,x) \\ f(0,1,0,0) = (1,1,1,2) = (y,y,y,2y) \\ f(0,0,1,0) = (-3,1,-5,-4) = (-3z,z,-5z,-4z) \\ f(0,0,0,1) = (2,4,1,5) = (2t,4t,t,5t) \end{cases}$

$\Rightarrow f(x,y,z,t) = (x+y-3z+2t, -x+y+z+4t, 2x+y-5z+t, x+2y-4z+5t)$.

5. $\varphi(e_1) = \varphi(1\cdot 1+0\cdot X+0\cdot X^2) = (1+0)+(0+0)X+(1+0)X^2 = 1+X^2$

$\varphi(e_2) = \varphi(0\cdot 1+1\cdot X+0\cdot X^2) = (0+1)+(1+0)X+(0+0)X^2 = 1+X$

$\varphi(e_3) = \varphi(0\cdot 1+0\cdot X+1\cdot X^2) = (0+0)+(0+1)X+(0+1)X^2 = X+X^2$

Then: $[\varphi]_E = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$

$\varphi(b_1) = \varphi(1\cdot 1+0\cdot X+0\cdot X^2) = (1+0)+(0+0)X+(1+0)X^2 = 1+X^2$

$\varphi(b_2) = \varphi(-1\cdot 1+1\cdot X+0\cdot X^2) = (-1+1)+(1+0)X+(-1+0)X^2 = X - X^2$

$\varphi(B_3) = \varphi(1\cdot 1+0\cdot X+1\cdot X^2) = (1+0)+(0+1)X+(1+1)X^2 = 1+X+2X^2$

Then: $[\varphi]_B = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & -1 & 2 \end{bmatrix}$

6. $det[f]_B = 1 \neq 0 \Rightarrow f$ is an automorphism $\Rightarrow [2f]_B = 2[f]_B = \begin{bmatrix} 2 & 4 \\ -2 & -2 \end{bmatrix}$.

$\begin{cases} f(v_1) = (1,-1) \\ f(v_2) = (2,-1) \end{cases} \Rightarrow \begin{cases} a_1x+b_1y = 1 \\ a_2x+b_2y = -1 \end{cases}$.

From $x=1, y=2 \Rightarrow \begin{cases} a_1+2b_1 = 1 \\ a_2+2b_2 = -1 \end{cases} \Rightarrow a_1 = -1$ and $a_2 = -1$.

From $x=1, y=3 \Rightarrow \begin{cases} a_1+3b_1 = 2 \\ a_2+3b_2 = -1 \end{cases} \Rightarrow b_1 = 1$ and $b_2 = 0$.

Hence, $f(x,y) = (y-x, -x)$.

$\begin{cases} g(v_1') = (-7,5) \\ g(v_2') = (-13,7) \end{cases} \Rightarrow \begin{cases} a_1x+b_1y = -7 \\ a_2x+b_2y = 5 \end{cases}$.

From $x = 1, y = 0 \Rightarrow a_1 = -7$ and $a_2 = 5$. From $x = 2, y = 1 \Rightarrow b_1 = 1$ and $b_2 = -3 \Rightarrow g(x, y) = (y - 7x, 5x - 3y)$.

Now, we compute $(f + g)(x, y) = f(x, y) + g(x, y) = (y - x, -x) + (y - 7x, 5x - 3y)$. And we apply this to the vectors v_1, v_2. So, $(f + g)(v_1) = (-4, -2)$ and $(f + g)(v_2) = (-2, -5) \Rightarrow [f + g]_B = \begin{bmatrix} -4 & -2 \\ -2 & -5 \end{bmatrix}$.

In the end, we compute $(f \circ g)(x, y) = f(g(x, y)) = (12x - 4y, -y + 7x)$ and we apply this to the vectors v'_1, v'_2. So, $(f \circ g)(v'_1) = (12, 7)$ and $(f \circ g)(v'_2) = (20, 13) \Rightarrow [f \circ g]_{B'} = \begin{bmatrix} 12 & 20 \\ 7 & 13 \end{bmatrix}$.

7. $f(e_1) = (cos(\alpha), sin(\alpha))$ and $f(e_2) = (-sin(\alpha), cos(\alpha))$.

   So, $[f]_E = \begin{bmatrix} cos(\alpha) & -sin(\alpha) \\ sin(\alpha) & cos(\alpha) \end{bmatrix}$.

   We compute $det([f]_E) = cos^2(\alpha) + sin^2(\alpha) = 1 \neq 0 \Rightarrow f$ is an automorphism.

8. $dim_{\mathbb{Z}_2}(V) = 2 \Rightarrow \mid V \mid = 2^2 = 4$ and $\mid M_2(\mathbb{Z}_2) \mid = 2^4 = 16$.

   As $End_{\mathbb{Z}_2}(V)$ is isomorphic to $M_2(\mathbb{Z}_2) \Rightarrow \mid End_{\mathbb{Z}_2}(V) \mid = 2^4$.

Seminar 11

$\forall v \in V : [v]_B = T_{BB'} \cdot [v]_{B'}$ and $T_{BB'}^{-1} = T_{B'B}$.
$[f]_{B'} = T_{BB'}^{-1} \cdot [f]_B \cdot T_{BB'}$.
$f(v) = \lambda \cdot v$, where λ is the eigenvalue and v is the eigenvector.
$p(\lambda) = (\lambda - \lambda_1)(\lambda - \lambda_2) = \lambda^2 - \lambda \cdot Tr(A) + det(A)$.

1. We want to determine $T_{BB'}$. So, we compute the vectors in B as a linear combination of vectors in B'.

   $v_1 = a_1 v_1 + a_2 v_2 + a_3 v_3 = (a_1 - a_2, a_1, a_3) = (1, 0, 1) \Rightarrow a_1 = 0$, $a_2 = -1$ and $a_3 = 1$.

   $v_2 = (a_1 - a_2, a_1, a_3) = (0, 1, 1) \Rightarrow a_1 = 1$, $a_2 = 1$ and $a_3 = 1$.

   $v_3 = (a_1 - a_2, a_1, a_3) = (1, 1, 1) \Rightarrow a_1 = 1$, $a_2 = 0$ and $a_3 = 1$.

   Hence, $T_{BB'} = \begin{bmatrix} 0 & 1 & 1 \\ -1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$ (on the columns). Now, we need $T_{B'B}$ which is actually $T_{BB'}^{-1}$. And by simple computations, we get that $T_{B'B} = \begin{bmatrix} -1 & 0 & 1 \\ -1 & 1 & 1 \\ 2 & -1 & -1 \end{bmatrix}$.

   Now, we have to find $[u]_{B'}$, which is $(2, 0, -1) = (a_1 - a_2, a_1, a_3) \Rightarrow$ $a_1 = 0$, $a_2 = -2$ and $a_3 = -1$. And, for $[u]_B$ we use the formula $[u]_B = T_{BB'} \cdot [u]_{B'} = \begin{bmatrix} -3 & -2 & -3 \end{bmatrix}$.

   We could also use $[u]_{B'} = T_{B'E} \cdot [u]_E$.

2. $v_1' = -3v_1 + 2v_2$ and $v_2' = -5v_1 + 3v_2$. So, $T_{B'B} = \begin{bmatrix} -3 & -5 \\ 2 & 3 \end{bmatrix}$. And, we know that $T_{B'B} = T_{BB'}^{-1}$, hence $T_{BB'} = \begin{bmatrix} 3 & 5 \\ -2 & -3 \end{bmatrix}$.

   Then, $[g]_B = T_{B'B}^{-1} \cdot [g]_{B'} \cdot T_{B'B} = \begin{bmatrix} -20 & -31 \\ 13 & 20 \end{bmatrix}$.

   Hence, $[f + g]_B = [f]_B + [g]_B = \begin{bmatrix} -19 & -30 \\ 12 & -19 \end{bmatrix}$.

   For $[f \circ g]_{B'} = [f]_{B'} \cdot [g]_{B'}$. We compute $[f]_{B'} = T_{BB'}^{-1} \cdot [f]_B \cdot T_{BB'} = \begin{bmatrix} 8 & 13 \\ -5 & -8 \end{bmatrix}$.

Hence, $[f \circ g]_{B'} = \begin{bmatrix} 9 & -13 \\ 5 & 9 \end{bmatrix}$.

3. Homework

4. (i) $f(e_1) = (3,2)$ and $f(e_2) = (3,4) \Rightarrow A = \begin{bmatrix} 3 & 3 \\ 2 & 4 \end{bmatrix} \Rightarrow det(A - \lambda I_2) = \begin{vmatrix} 3-\lambda & 3 \\ 2 & 4-\lambda \end{vmatrix} = 0 \iff (\lambda - 3)(\lambda - 4) = 6 \iff \lambda^2 - 7\lambda + 6 = 0 \Rightarrow \lambda_1 = 1$ and $\lambda_2 = 6$.
Take $\begin{bmatrix} 3-\lambda & 3 \\ 2 & 4-\lambda \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$.
For $\lambda_1 = 1 \Rightarrow 2x_1 + 3x_2 = 0 \Rightarrow x_1 = -\frac{3}{2}x_2 \Rightarrow V(1) = \{(-\frac{3}{2}x_2, x_2) \mid x_2 \in \mathbb{R}\} =< (\frac{3}{2}, 1) >$.
For $\lambda_2 = 6 \Rightarrow 2x_1 - 2x_2 = 0 \Rightarrow x_1 = x_2 \Rightarrow V(6) = \{(x_2, x_2) \mid x_2 \in \mathbb{R}\} =< (1,1) >$.
(ii) As $dim(\mathbb{R}^2) = 2$, where $f \in End_{\mathbb{R}}(\mathbb{R}^2)$ and $\lambda_1 \neq \lambda_2 \Rightarrow B =< (\frac{3}{2}, 1), (1,1) >$ is a basis and $[f]_B = \begin{bmatrix} 1 & 0 \\ 0 & 6 \end{bmatrix}$.

5. $\begin{vmatrix} 3-\lambda & 1 & 0 \\ -4 & -1-\lambda & 0 \\ -4 & -8 & -2-\lambda \end{vmatrix} = 0 \iff (2+\lambda)[(\lambda+1)(3-\lambda) - 4] = 0 \Rightarrow \lambda_1 = -2$ and $\lambda_2 = \lambda_3 = 1$.
For $\lambda_1 = -2 \Rightarrow \begin{bmatrix} 5 & 1 & 0 \\ -4 & 1 & 0 \\ -4 & -8 & 0 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = O_3 \Rightarrow \begin{cases} 5x_1 + x_2 = 0 \\ -4x_1 + x_2 = 0 \\ -4x_1 - 8x_2 = 0 \end{cases} \Rightarrow$
$x_1 = -2x_2 \Rightarrow V(-2) = \{(-2x_2, x_2, x_3) \mid x_2, x_3 \in \mathbb{R}\} =< (-2,1,0), (0,0,1) >$.
For $\lambda_2 = \lambda_3 = 1 \Rightarrow \begin{bmatrix} 2 & 1 & 0 \\ -4 & -2 & 0 \\ -4 & -8 & -3 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = O_3 \Rightarrow \begin{cases} 2x_1 + x_2 = 0 \\ -4x_1 - 8x_2 = 0 \end{cases} \Rightarrow$
$-2x_1 = x_2$ and $x_3 = 4x_1 \Rightarrow V(1) = \{(x_1, -2x_1, 4x_1) \mid x_1 \in \mathbb{R}\} =< (1, -2, 4) >$.

6. $\begin{vmatrix} -\lambda & 0 & 0 & 1 \\ 0 & -\lambda & 1 & 0 \\ 0 & 1 & -\lambda & 0 \\ 1 & 0 & 0 & -\lambda \end{vmatrix} = 0 \iff (\lambda - 1)(\lambda + 1)(\lambda^2 + 1) = 0 \Rightarrow \lambda_1 = 1$, $\lambda_2 = -1$, $\lambda_3 = i$ and $\lambda_4 = -i$.

For $\lambda_1 = 1$ we have the system $\begin{cases} -x_1 + x_4 = 0 \\ -x_2 + x_3 = 0 \end{cases} \Rightarrow x_1 = x_4$ and $x_2 = x_3 \Rightarrow V(1) = \{(x_1, x_2, x_2, x_1) \mid x_1, x_2 \in \mathbb{R}\} =< (1,0,0,1), (0,1,1,0) >$.

For $\lambda_2 = -1$ we have the system $\begin{cases} x_1 + x_4 = 0 \\ x_2 + x_3 = 0 \end{cases} \Rightarrow x_1 = -x_4$ and $x_2 = -x_3 \Rightarrow V(-1) = \{(x_1, x_2, -x_2, -x_1) \mid x_1, x_2 \in \mathbb{R}\} =< (1,0,0,-1), (0,1,-1,0) >$.

For $\lambda_3 = i$ we have the system $\begin{cases} x_1 - ix_4 = 0 \\ x_2 - ix_3 = 0 \end{cases} \Rightarrow x_1 = ix_4$ and $x_2 = ix_3 \Rightarrow V(i) = \{(ix_4, ix_3, x_3, x_4) \mid x_3, x_4 \in \mathbb{R}\} =< (i,0,0,1), (0,i,1,0) >$.

For $\lambda_4 = -i$ we have the system $\begin{cases} ix_1 + x_4 = 0 \\ ix_2 + x_3 = 0 \end{cases} \Rightarrow -ix_1 = x_4$ and $-ix_2 = x_3 \Rightarrow V(-i) = \{(x_1, x_2, -ix_2, -ix_1) \mid x_1, x_2 \in \mathbb{R}\} =< (1,0,0,-i), (0,1,-i,0) >$.

7. $\begin{vmatrix} x-\lambda & 0 & y \\ 0 & x-\lambda & 0 \\ y & 0 & x-\lambda \end{vmatrix} = 0 \iff (x-\lambda)(x-\lambda-y)(x-\lambda+y) = 0 \Rightarrow$
$\lambda_1 = x$, $\lambda_2 = x - y$ and $\lambda_3 = x + y$.

For $\lambda_1 = x$ we have the system $\begin{cases} yx_3 = 0 \\ yx_1 = 0, y \neq 0 \end{cases} \Rightarrow x_1 = x_3 = 0 \Rightarrow V(x) = \{(0, x_2, 0) \mid x_2 \in \mathbb{R}\} =< (0,1,0) >$.

For $\lambda_2 = x - y$ we have the system $\begin{cases} yx_1 + yx_3 = 0 \\ yx_2 = 0, y \neq 0 \end{cases} \Rightarrow x_1 = -x_3$ and $x_2 = 0 \Rightarrow V(x-y) = \{(-x_3, 0, x_3) \mid x_3 \in \mathbb{R}\} =< (-1,0,1) >$.

For $\lambda_3 = x + y$ we have the system $\begin{cases} -yx_1 + yx_3 = 0 \\ -yx_2 = 0, y \neq 0 \end{cases} \Rightarrow x_1 = x_3$ and $x_2 = 0 \Rightarrow V(x+y) = \{(x_1, 0, x_1) \mid x_1 \in \mathbb{R}\} =< (1,0,1) >$.

8. Homework

9. (i) $p(\lambda) = det(A - \lambda I_2)$, where $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \Rightarrow p(\lambda) = \lambda^2 - \lambda(a+d) + (ad - bc)$.

Now, $p(0) = det(A - 0 \cdot I_2) = det(A) = 0^2 - 0 \cdot (a + d) + ad - bc$. As λ_1, λ_2 are eigenvalues $\Rightarrow p(\lambda) = (\lambda - \lambda_1)(\lambda - \lambda_2) = \lambda^2 - \lambda(\lambda_1 + \lambda_2) + \lambda_1 \cdot \lambda_2$. Also, $p(0) = (0 - \lambda_1)(0 - \lambda_2) = \lambda_1 \cdot \lambda_2 = det(A)$.

Hence, $\lambda_1 + \lambda_2 = a + d = Tr(A)$.

(ii) $\lambda^2 - \lambda(\lambda_1 + \lambda_2) + \lambda_1 \cdot \lambda_2 = \lambda^2 - \lambda \cdot Tr(A) + det(A) = 0 \Rightarrow \Delta = (Tr(A))^2 - 4det(A)$. If $0 \leq \Delta \Rightarrow \exists \lambda_1, \lambda_2 \in \mathbb{R}$ with $\lambda_1 = \lambda_2$ or $\lambda_1 \neq \lambda_2$.

If $\exists \lambda_1, \lambda_2 \in \mathbb{R} \Rightarrow 0 \leq \Delta$.

(iii) For A to be aroot of $p(\lambda)$, $p(A) = O_2 \iff A^2 - A \cdot Tr(A) + I_2 \cdot det(A) = O_2 \iff \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} - (a + d) \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} + (ad - bc) \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = O_2$, which, by simple computations, we get that is true.

10. $det(A - iI_2) = 0 = p(i)$, where $p(i) = (i - \lambda_1)(i - \lambda_2) = -1 - i \cdot Tr(A) + det(A) = 0 \Rightarrow det(A) = 1 + i \cdot Tr(A)$.

Now $det(A - 2I_2) = 4 - 2Tr(A) + det(A)$, so $det(A - 2I_2) = 4 - 2Tr(A) + 1 + iTr(A) = 5 + (i - 2)Tr(A)$.

From $det(A) = 1 + iTr(A)$, we have that $det(A), Tr(A), 1 \in \mathbb{R} \Rightarrow Tr(A) = 0$.

Hence, $det(A - 2I_2) = 5$.

Seminar 12

(3,2)-party check code is a 2-digits message, with a 3-digits code, where the first digit is the sum of the 2 digits of the message, computed modulo 2.

(3,1)-repeating code is a 1-digit message, with a 3-digits code, where the first and the second digits repeat the code.

$p \in \mathbb{Z}_2[X]$ of degree $n-k$ is a generator of a polynomial code (n,k), whose words are polynomials of degree less then n, divisible by p.

For a (n,k) polynomial code, we have 2^k code words. For a message m, we transform it as $m \cdot X^{n-k} = qp + r$, where $degree(r) < degree(p) = n-k$. And we code it as $v = r + m \cdot X^{n-k}$.

A **party check matrix** looks like $H = (I_{n-k} \mid P)$. And a vector $u \in M_{n,1}(\mathbb{Z}_2)$ is a code vector $\iff H \cdot u = 0$.

Hamming distance: u, v of the same length $\Rightarrow$ the number of positions in which they differ. We denote it by $d(u,v)$, which is a metric on $\mathbb{Z}_2^n$.

A code detects all erros $\leq t \iff min(d(u,v)) \geq t+1$. And it can correct all errors $\leq t \iff min(d(u,v)) \geq 2t+1$.

An **enconder** is $\gamma : \mathbb{Z}_2^k \to \mathbb{Z}_2^n$ with $[\gamma]_{EE'} = G$.

1. (i) $110 \to 1 = (1+0) \pmod 2$. This is true, so it does not have detectable errors.

   $010 \to 0 = (1+0) \pmod 2$. This is not true, so it contains a detectable error.

   The same goes for all, so the words with detectable errors are :$010, 001, 111$.

   (ii) $111 \to 11$ repeat the message 1.

   $011 \to 01$ repeat the message 1.

   The same for all, except the last one $001 \to 00$ does not repeat the message 1.

2. Let $f = X^7 + X^6 + X^4 + X^3 + 1$ and $g = X^6 + X^3 + X^2 + X$.

   We have the code $(8,4)$, so $n = 8$ and $k = 4$.

   We compute $f : p$, which gives us the quotient $X^3 + X$ and the reminder $X^3 + X + 1$. So f is not divisible by p, hence f is not a code word.

   We compute $g : p$, which gives us the quotient $X^2 + X$ and no reminder. So $p \mid g$, hence g is a code word.

3. For the code $(6, 3)$ we have $n = 6$ and $k = 3$.

   We have $2^k = 2^3 = 8$ words $\Rightarrow$ The messages are $\{000, 001, 010, 100, 011, 101, 110, 111\}$.

   We take the first word $000 = m$. We compute $m = 0{\cdot}X^0{+}0{\cdot}X^1{+}0{\cdot}X^2 = 0$. So $m \cdot X^{n-k} = 0$.

   Now, we compute $r = m \cdot X^{n-k} \pmod{p} \Rightarrow r = 0$.

   And, in the end $v = r + m \cdot X^{n-k} \Rightarrow v = 0 \Rightarrow 000000$ (the same number of digits as n).

   We do this for all words and we get:

   $001 \to m = 0 \cdot X^0 + 0 \cdot X^1 + 1 \cdot X^2 \to mX^{n-k} = X^5 \to r = X + 1 \to v = 1 + X + X^5 \to 110001$

   $010 \to mX^{n-k} = X^4 \to r = X^2 + X + 1 \to v = 1 + X + X^2 + X^4 \to 111010$

   $100 \to mX^{n-k} = X^3 \to r = X^2 + 1 \to v = 1 + X^2 + X^3 \to 111000$

   $011 \to mX^{n-k} = X^4 + X^5 \to r = X + 1 \to v = X^5 + X + 1 \to 110001$

   $101 \to mX^{n-k} = X^3 + X^5 \to r = X^2 + X \to v = X + X^2 + X^3 + X^5 \to 011101$

   $110 \to mX^{n-k} = X^3 + X^4 \to r = X \to v = X + X^3 + X^4 \to 010110$

   $111 \to mX^{n-k} = X^3 + X^4 + X^5 \to r = 1 \to v = 1 + X^3 + X^4 + X^5 \to 100111$

4. We have $n = 5$ and $k = 3$ and $H = (I_{n-k} \mid P) \Rightarrow H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix}$.

   For a vector $u = (u_1, u_2, u_3, u_4, u_5)$ we need to solve the system $H \cdot u = O_2$.

   So, we get the system $\begin{cases} u_1 + u_5 = 0 \\ u_2 + u_3 + u_4 + u_5 = 0 \end{cases}$

   $\Rightarrow u = (u_2 + u_3 + u_4, u_2, u_3, u_4, u_2 + u_3 + u_4)$

   $\Rightarrow \{(0,0,0,0,0), (1,1,0,0,1), (1,0,1,0,1), (1,0,0,1,1), (0,1,1,0,0,), (0,0,1,1,0), (0,1,0,1,0), (1,1,1,1,1)\}$.

5. We compute $H = (I_5 \mid P) \Rightarrow H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$.

For a vector $u = (u_1, u_2, \dots, u_9)$, we compute $H \cdot u = O_9$ and we solve the system that forms.

In the end, we get the vector:

$u = (u_8, u_7 + u_9, u_6 + u_8 + u_9, u_7, u_6 + u_9, u_6, u_7, u_8, u_9)$.

$\Rightarrow \{000000000, 001011000, 010100100, 101000010, 011010001, 011111100, 100011010, 010001001, 111100110, 001110101, 110010011, 110111110, 000101101, 111001011, 100110111\}$.

Now, for the Hamming distance we need $min(d(u_i, u_j))$. For that, we must compute $min(d(u_1, u_i)) = min(d(u_2, u_i)) = \dots = min(d(u_9, u_i)) = 3$.

As $min(d(u_i, u_j)) = 3 \geq t + 1 \Rightarrow t \leq 2 \Rightarrow$ the code detects 2 errors.

And, as $min(d(u_i, u_j)) = 3 \geq 2t + 1 \Rightarrow t \leq 1 \Rightarrow$ the code can correct 1 error.

6. From $G = [\gamma]_{EE'} \Rightarrow \begin{cases} \gamma(e_1) = 001011000, e_1 = 1000 \\ \gamma(e_2) = 010100100, e_2 = 0100 \\ \gamma(e_3) = 101000010, e_3 = 0010 \\ \gamma(e_4) = 011010001, e_4 = 0001 \end{cases}$

For $1101 = e_1 + e_2 + e_4 \Rightarrow \gamma(1101) = \gamma(e_1) + \gamma(e_2) + \gamma(e_4) = 001011000 + 010100100 + 011010001 = 000101101$.

For $0111 = e_2 + e_3 + e_4 \Rightarrow \gamma(0111) = \gamma(e_2) + \gamma(e_3) + \gamma(e_4) = 100110111$.

For $0000 = e_1 + e_2 \Rightarrow \gamma(0000) = \gamma(e_1) + \gamma(e_2) = 000000000$.

For $1000 = e_1 \Rightarrow \gamma(1000) = \gamma(e_1) = 001011000$.

7. We have $\gamma : \mathbb{Z}_2^1 \to \mathbb{Z}_2^4$, with $[\gamma]_{EE'} = G$, where $E = (e_1) = 1$ and $E' = (e_1', e_2', e_3', e_4')$.

For $e_1 = 1 \Rightarrow m = 1 \Rightarrow mX^{n-k} = X^3 \Rightarrow r = X^2 + X + 1 \Rightarrow v = 1 + X + X^2 + X^3 \Rightarrow 1111$.

Hence, $G = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} P \\ I_k \end{bmatrix} \Rightarrow P = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$.

Now, $H = (I_{n-k} \mid P) = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$.

8. We have $\gamma : \mathbb{Z}_2^3 \to \mathbb{Z}_2^7$, with $[\gamma]_{EE'} = G$, where $E = (e_1, e_2, e_3)$ and $E' = (e'_1, e'_2, e'_3, e'_4, e'_5, e'_6, e'_7)$.

   For $e_1 = (1, 0, 0) \Rightarrow 100 \Rightarrow m = 1 \Rightarrow mX^{n-k} = X^4 \Rightarrow r = 1 + X^2 + X^3 \Rightarrow v = 1 + X^2 + X^3 + X^4 \Rightarrow 1011100$.

   For $e_2 = (0, 1, 0) \Rightarrow 010 \Rightarrow m = X \Rightarrow mX^{n-k} = X^5 \Rightarrow r = 1 + X^2 \Rightarrow v = 1 + X + X^2 + X^5 \Rightarrow 1110010$.

   For $e_3 = (0, 0, 1) \Rightarrow 001 \Rightarrow m = X^2 \Rightarrow mX^{n-k} = X^6 \Rightarrow r = X + X^2 + X^3 \Rightarrow v = X + X^2 + X^3 + X^6 \Rightarrow 0111001$.

   Hene, $G = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \Rightarrow P = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \Rightarrow H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$.