Problem session February 20, 2023

(Group algebras)

1. Show that these $\mathbb{F}$-algebras are isomorphic:

   a) $\mathbb{F}G \simeq \mathbb{F}[x]/(x^n - 1)$, where G is a cyclic group of order $n \in \mathbb{N}$.

   b) $\mathbb{F}G \simeq \mathbb{F}[x,y]/(x^2 - 1, y^2 - 1)$, where $G = \mathbb{Z}_2 \times \mathbb{Z}_2$.

Solution

a) Let $G = \mathbb{Z}_n$, so $\{\delta_g \mid g = 0, 1, \dots, n-1\}$ is a basis of $\mathbb{F}G$.

It is easy to verify that for every $\mathbb{F}$-algebra A and for every $a \in A$ there exists a unique homomorphism of $\mathbb{F}$-algebras $\varphi\colon \mathbb{F}[x] \to A$ satisfying $\varphi(x) = a$.

We will not prove it here but the only possible definition is $\varphi(h) := h(a)$ for each $h \in \mathbb{F}[x]$. That is, if $h = \sum_{i=0}^m f_i x^i \in \mathbb{F}[x]$, then $\varphi(h) = \sum_{i=0}^m f_i a^i$. It remains to check that φ is a homomorphism of $\mathbb{F}$-algebras.

We apply this fact for $A = \mathbb{F}G$ and $a = \delta_1$. We get a homomorphism of $\mathbb{F}$-algebras $\varphi\colon \mathbb{F}[x] \to \mathbb{F}G$ which maps x^i to $\delta_{i \bmod n}$. Since $\mathrm{Im}\ \varphi$ contains a basis of $\mathbb{F}G$, φ has to be onto. It remains to find $\mathrm{Ker}\ \varphi$.

Note that $\varphi(x^n - 1) = \delta_0 - \delta_0 = 0$. Therefore $x^n - 1 \in \mathrm{Ker}\ \varphi$. It means $\mathrm{Ker}\ \varphi$ is an ideal of $\mathbb{F}[x]$ generated by a divisor of $x^n - 1$. Since $\mathbb{F}G = \mathrm{Im}\ \varphi = \mathbb{F}[x]/\mathrm{Ker}\ \varphi$ has dimension n, we get $\mathrm{Ker}\ \varphi = (x^n - 1)$ and $\mathbb{F}G \simeq \mathbb{F}[x]/(x^n - 1)$ follows.

b) A similar approach can be applied also in this case but we present another type of argument, which is somewhat 'brute force style'.

First assume that A, B are two $\mathbb{F}$-algebras and $\varphi\colon A \to B$ is a map such that

1. $\varphi \in \mathrm{Hom}_{\mathbb{F}}(A, B)$,
2. $\varphi(1_A) = 1_B$,
3. there exists a basis $X \subseteq A$ such that $\varphi(x_1 x_2) = \varphi(x_1)\varphi(x_2)$ for every $x_1, x_2 \in X$.

Then φ is a homomorphism of $\mathbb{F}$-algebras.

To check this observation, we assume for simplicity that X is finite and that $a = \sum_{x \in X} f_x x$, $a' = \sum_{x \in X} f'_x x$ are elements of A. Then $\varphi(aa') = \varphi(\sum_{x,x' \in X} f_x f'_{x'} x x') = \sum_{x,x'} f_x f'_{x'} \varphi(xx') = \sum_{x,x'} f_x \varphi(x) f_{x'} \varphi(x') = \varphi(a)\varphi(a')$. That is, φ is indeed compatible with the multiplication.

Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (1,0), (0,1), (1,1)\}$. We consider a basis $X = \{\delta_g \mid g \in G\}$ of this algebra.

Then we define a linear map $\varphi\colon \mathbb{F}G \to \mathbb{F}[x,y]/(x^2 - 1, y^2 - 1)$ by

$$\varphi(\delta_{0,0}) = \overline{1}, \varphi(\delta_{1,0}) = \overline{x}, \varphi(\delta_{0,1}) = \overline{y}, \varphi(\delta_{1,1}) = \overline{xy}$$

Since $\varphi(\delta_0) = \overline{1}$, condition 2. is satisfied.

A bit tedious is the verification of 3. But notice that $\overline{x}^2 = \overline{y}^2 = (\overline{xy})^2 = \overline{1}$. And if α, β are two different elements of $\{\overline{x}, \overline{y}, \overline{xy}\}$ then $\alpha\beta$ is the third element of this set. Using these observations we check condition 3. easily.

Finally note that φ is onto and $\dim_{\mathbb{F}}(\mathbb{F}G) = 4 = \dim_{\mathbb{F}}\mathbb{F}[x,y]/(x^2-1, y^2-1)$, so φ is indeed an isomorphism of $\mathbb{F}$-algebras.

2. For which groups is the group algebra $\mathbb{F}G$ commutative?

Solution: If $\mathbb{F}G$ is commutative $\mathbb{F}$-algebra, then $\delta_{gh} = \delta_g * \delta_h = \delta_h * \delta_g = \delta_{hg}$ for every $g, h \in G$. So G has to be a commutative group.

Conversely, it is easy to see that an $\mathbb{F}$-algebra is commutative provided it has a basis B such that $b_1b_2 = b_2b_1$ for every $b_1, b_2 \in B$.

Indeed, let $\alpha = \sum_{b\in B} f_b b$ and $\beta = \sum_{b\in B} f'_b b$ where only finitely many coefficients $f_b, f'_b \in \mathbb{F}$ are nonzero. Let $B_0 \subseteq B$ be a finite set such that $\alpha = \sum_{b\in B_0} f_b b$ and $\beta = \sum_{b\in B_0} f'_b b$. Since the elements of B_0 commute with each other, $\alpha\beta = \sum_{b,b'\in B_0} f_b f_{b'} bb' = \sum_{b,b'\in B_0} f_{b'} f_b b' b = \beta\alpha$.

Now assume that G is a commutative group. Then $B = \{\delta_g \mid g \in G\}$ is a basis of $\mathbb{F}G$ such that $\delta_g * \delta_h = \delta_h * \delta_g$ for every δ_g, δ_h. So the general principle explained above applies here.

The conclusion of this exercise is: $\mathbb{F}G$ is a commutative $\mathbb{F}$-algebra if and only if G is a commutative group.

3. For which finite groups is the group algebra $\mathbb{F}G$ field?

Solution: We will use a well-known theorem (I hope it is still tought in some course) - every finite subgroup of the multiplicative group of a field is cyclic. So $\mathbb{F}G$ can be a field only if G is a cyclic group. On the other hand, using the result of the first exercise, if G is a cyclic group of order n, then $\mathbb{F}G \simeq \mathbb{F}[x]/(x^n-1)$. So we are left to answer for which $n \in \mathbb{N}$ $x^n - 1 \in \mathbb{F}[x]$ is irreducible. The factorization $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$ gives the answer - $x^n - 1$ is irreducible only if $n = 1$.

The conclusion of this exercise is: If G is a finite group and $\mathbb{F}$ is a field, then $\mathbb{F}G$ is a field of and only if $G = 1$. In this case $\mathbb{F}G \simeq \mathbb{F}$.

Remark: Note that in fact we proved that if G contains an element of finite order different from 1, then $\mathbb{F}G$ is not an integral domain.

Remark: When writing this solution I realized there is an easier argument which works also for infinite groups. If G is a nontrivial group then $\mathbb{F}G$ has a proper two-sided ideal (called the augmentation ideal)

$$I = \{\sum_{g\in G} t_g\delta_g \in \mathbb{F}G \mid \sum_{g\in G} t_g = 0\}$$

So if $G \neq 1$, then $\mathbb{F}G$ cannot be a field.

(Invariant subspaces)

4. Let $G = S_3$, let $\mathbb{F}$ be a field. Consider the following action G on $V := \mathbb{F}^3$.

$$g * (x_1, x_2, x_3)^T := (x_{g^{-1}(1)}, x_{g^{-1}(2)}, x_{g^{-1}(3)})^T, g \in S_3, (x_1, x_2, x_3)^T \in V$$

This action gives a representation $\varphi\colon G \to \mathrm{Aut}_{\mathbb{F}}(V)$ given by

$$\varphi(g)\colon v \mapsto g * v, g \in G, v \in V$$

a) Check that φ is really a representation of G.

b) Give examples of some φ-invariant subspaces.

c) Find all φ-invariant subpaces if $\mathrm{char}(\mathbb{F}) \neq 2, 3$.

d) Try to find all φ-invariant subspaces if $\mathbb{F} = \mathbb{F}_2$.

e) Try to find all φ-invariant subspaces if $\mathbb{F} = \mathbb{F}_3$.

(parts d),e) are cases when $\mathrm{char}(\mathbb{F}) \mid |G|$. In representation theory such representations are called modular and the theory for modular representations is more complicated that the one which we are going to learn during our lectures).

Solution

a) Obviously $\varphi(g) \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{F}^3)$ for every $g \in S_3$. We need to check that $\varphi\colon S_3 \to \mathrm{Aut}_{\mathbb{F}}(\mathbb{F}^3)$ is a homomorphism of groups. Let $e_1 = (1,0,0)^T, e_2 = (0,1,0)^T, e_3 = (0,0,1)^T$ be the canonical basis of $\mathbb{F}^3$. If $g \in S_3$ then

$$[\varphi(g)](\sum_{i=1}^{3} x_i e_i) = \sum_{i=1}^{3} x_i e_{g(i)} \,.$$

And if $h \in S_3$, then

$$[\varphi(h) \circ \varphi(g)](\sum_{i=1}^{3} x_i e_i) = [\varphi(h)](\sum_{i=1}^{3} x_i e_{g(i)}) = \sum_{i=1}^{3} x_i e_{h(g(i))} \,.$$

On the other hand $\varphi(hg)(\sum_{i=1}^{3} x_i e_i) = \sum_{i=1}^{3} x_i e_{h(g(i))}$.

So $\varphi(h) \circ \varphi(g) = \varphi(hg)$ for every $g, h \in G$, i.e, φ is indeed a homomorphism of groups.

b) For sure 0 and $V = \mathbb{F}^3$ are φ-invariant subspaces. Another example is $U = \{(t,t,t)^T \mid t \in \mathbb{F}\}$ since for any $g \in G$ and for any $u \in U$ we have $[\varphi(g)](u) = u$. Note that $\varphi_U\colon S_3 \to \mathrm{Aut}_{\mathbb{F}}(U)$ is a trivial representation of S_3 over $\mathbb{F}$. That is, $\dim_{\mathbb{F}}(U) = 1$ and $\varphi_U(g) = 1_U$ for every $g \in S_3$.

c),d) Consider $W = \{(x_1, x_2, x_3)^T \in \mathbb{F}^3 \mid x_1 + x_2 + x_3 = 0\}$. Obviously W is a φ-invariant subspace, since if $w = (x_1, x_2, x_3)^T \in W$ and $g \in S_3$, then $g * w = (x_{g^{-1}(1)}, x_{g^{-1}(2)}, x_{g^{-1}(3)}) \in W$.

We claim that $\varphi_W \in S_3 \to \mathrm{Aut}_{\mathbb{F}}(W)$ is irreducible. Let W' be a φ_W-invariant subspace of W (notice that it is the same as saying that W' is a φ-invariant subspace contained in W). Assume $0 \neq (x_1, x_2, x_3)^T \in W'$. Note that either $x_1 \neq x_2$ or $x_1 \neq x_3$. Since for any $g \in S_3$ the element $(x_{g^{-1}(1)}, x_{g^{-1}(2)}, x_{g^{-1}(3)}) \in W'$, we may assume $x_1 \neq x_2$. Then

$$(x_1, x_2, x_3)^T \in W'$$

$$(1,2) * (x_1, x_2, x_3)^T = (x_2, x_1, x_3)^T \in W'$$

$$(x_1 - x_2, x_2 - x_1, 0)^T \in W'$$

So W' contains $(1, -1, 0)^T$ and also $(0, 1, -1)^T = (1, 2, 3) * (1, -1, 0)^T$. But notice that $\{(1, -1, 0)^T, (0, 1, -1)^T\}$ is a basis of W, so $W' = W$.

Therefore every non-zero φ_W-invariant subspace of W is equal to W.

We claim that the only φ-invariant subspaces are $0, U, W, V$. Assume that W' is a φ-invariant subspace of V, $W' \notin \{0, U, W, V\}$. Since φ_W is irreducible, $W' \cap W = 0$ (otherwise $W' \cap W$ would be a non-trivial φ_W-invariant subspace of W). But then $W' \oplus W = \mathbb{F}^3$. Note that this implies $\dim_{\mathbb{F}}(W') = 1$. If we consider the factor representation $\overline{\varphi_W}\colon S_3 \to \mathrm{Aut}_{\mathbb{F}}(\mathbb{F}^3/W)$ we get a representation equivalent to φ_U. It means that every element of S_3 acts as the identity on W'. But every vector which is fixed by every element of S_3 has to be of the form $(t, t, t)^T$ for some $t \in \mathbb{F}$. It follows that $W' = U$. (An argument avoiding the use of a factor representation can be for example this: Write $w' \in W'$ as $w' = u + w, u \in U, w \in W$. For every $\pi \in S_3$ is $\pi * w' - w' = \pi * u + \pi * w - u - w = \pi * w - w$, i.e., $\pi * w' - w' \in W' \cap W = 0$).

e) Again we have φ-invariant subspaces $0, U, W, V$, where $U := \{(t, t, t)^T \mid t \in \mathbb{F}\}$ and $W := \{(x_1, x_2, x_3)^T \in \mathbb{F}^3 \mid x_1 + x_2 + x_3 = 0\}$. We claim that there is no other φ-invariant subspace but the argument has to be different since $t + t + t = 0$ (because of $\mathrm{char}(\mathbb{F}) = 3$) and hence $U \subseteq W$.

Consider a nonzero φ-invariant subspace $W' \leq V$. We distinguish 2 cases:

case 1: $W' \not\subseteq W$: take $(x_1, x_2, x_3)^T \in W' \setminus W$, that is $x_1 + x_2 + x_3 \neq 0$. Then

$$(x_1, x_2, x_3)^T + (1, 2, 3) * (x_1, x_2, x_3)^T + (1, 3, 2) * (x_1, x_2, x_3)^T =$$

$$(x_1, x_2, x_3)^T + (x_3, x_1, x_2)^T + (x_2, x_3, x_1)^T = (x_1 + x_2 + x_3)(1, 1, 1)^T \in W'$$

We got $(1, 1, 1)^T \in W'$ and also $(x_1, x_2, x_3)^T - x_1(1, 1, 1)^T = (0, x_2', x_3')^T \in W' \setminus W$. Note that $x_2' + x_3' \neq 0$. Then also $(x_2' + x_3')(0, 1, 1)^T = (0, x_2', x_3')^T + (2, 3) * (0, x_2', x_3')^T \in W'$. We got $(1, 1, 1)^T, (0, 1, 1)^T \in W'$, hence also $(1, 0, 0)^T = (1, 1, 1)^T - (0, 1, 1)^T \in W'$. And then $(0, 1, 0)^T = (1, 2, 3) * (1, 0, 0)^T \in W'$ and $(0, 0, 1)^T = (1, 3, 2) * (1, 0, 0)^T \in W'$.

So in if W' is not contained in W, then $W' = V$ (since it contains a basis of V).

case 2: Assume $W' \subseteq W$. If $W' \subseteq U$, then $W' = U$ since $0 \neq W'$ and U has dimension 1. Assume $W' \not\subseteq U$ and let $(x_1, x_2, x_3)^T \in W'$ be such that $x_1 \neq x_2$ (we can get such an element by permutation of coordinates of an arbitrary element of $W' \setminus U$). Then

$$(x_3, x_2, x_1)^T = (1, 3) * (x_1, x_2, x_3)^T \in W', (x_1, x_3, x_2)^T = (2, 3) * (x_1, x_2, x_3)^T \in W'$$

Then also $(2x_1 + x_3, 2x_2 + x_3, x_1 + x_2 + x_3)^T = (2x_1 + x_3, 2x_2 + x_3, 0)^T \in W'$. Note that $2x_1 + x_3 = x_1 - x_2$ and $2x_2 + x_3 = x_2 - x_1$. Then $(2x_1 + x_3, 2x_2 + x_3, 0)^T = (x_1 - x_2)(1, -1, 0)^T \in W'$. So we got that $(1, -1, 0)^T$ and also $(0, 1, -1)^T = (1, 2, 3) * (1, -1, 0)^T$ are in W'. That is $W' = W$.

Remark: Another approach for case 2 could be to realize that if $0 \neq W' \neq W$ then W' has dimension 1 and to be a φ-invariant it has to be a common eigenspace to all automorphism of the set $\{\varphi(g) \mid g \in S_3\}$. Then it is easy to see that every common eigenvector of this set has to be of the form $(t,t,t), t \in \mathbb{F}$, so $W' = U$. This observation could also simplify the solution of c) and d), since the irreducibility of φ_W is an immediate consequence of it.

5. (Some module theory) Show that every module over $\mathbb{F}[x]/(x^2)$ is isomorphic to a direct sum of cyclic modules.

Solution: Let M be an arbitrary left $R = \mathbb{F}[x]/(x^2)$-module. Consider the following sets

$$M_0 = \{m \in M \mid \overline{x}m = 0\}, M_1 = \overline{x}M = \{m \in M \mid \exists m' \in M \ m = \overline{x}m'\}$$

Since $\overline{x}^2 = 0$, $M_1 \subseteq M_0$

Note that every $\mathbb{F}$-subspace of M_0 is actualy an R-submodule of M_0 since for every $\alpha, \beta \in \mathbb{F}$ and for every $m \in M_0$ is $(\alpha + \beta\overline{x})m = \alpha m \in \mathbb{F}m$.

Choose an arbitrary basis B_1 of M_1 and extend this basis to a basis of M_0. $B = B_1 \dot{\cup} B_0$ is a basis of M_0. For every $b \in B_1$ fix an element $m_b \in M$ such that $\overline{x}m_b = b$.

We claim that

$$M = (\oplus_{b \in B_1} Rm_b) \oplus (\oplus_{b \in B_0} Rb)$$

First we check that M is generated by the set $\{m_b \mid b \in B_1\} \cup B_0$. Let M' be the submodule of M generated by $\{m_b \mid b \in B_1\} \cup B_0$. Since every $m \in M_0$ is a linear combination of elements from the set $\{\overline{x}m_b \mid b \in B_1\} \cup B_0$, $M_0 \subseteq M'$.

If $m \in M$, then $\overline{x}m \in M_1$ so there exists $m' \in M'$ (in fact a linear combination of elements from $B_1 = \{\overline{x}m_b \mid b \in B_1\}$) such that $\overline{x}m = m'$. Assume that $m' = \sum_{b \in B_1} t_b \overline{x} m_b$ for some $t_b \in \mathbb{F}$. Put $m_1 := \sum_{b \in B_1} t_b m_b$. Then $\overline{x}(m - m_1) = 0$, that is $m - m_1 \in M_0 \subseteq M'$. Hence also $m \in m_1 + M_0 \subseteq M'$.

To conclude the proof we check that if $\sum_{b \in B_1} r_b m_b + \sum_{b \in B_0} r_b b = 0$ for some $r_b \in R$, where only finitely many of r_b's are nonzero, then necessarily $r_b m_b = 0$ for every $b \in B$. We check this in two steps

1. Look at $\overline{x}(\sum_{b \in B_1} r_b m_b + \sum_{b \in B_0} r_b b) = 0$ which is equivalent to $\sum_{b \in B_1} r_b b = 0$. For every $b \in B_1$ write r_b as $\alpha_b + \beta_b \overline{x}$ for some $\alpha_b, \beta_b \in \mathbb{F}$. The linear independence of B_1 together with $r_b b = \alpha_b b$ gives $\alpha_b = 0$ for every $b \in B_1$.

2. For every $b \in B_1$ write $r_b = \beta_b \overline{x}$ for some $\beta_b \in \mathbb{F}$ and substitute this to $\sum_{b \in B_1} r_b m_b + \sum_{b \in B_0} r_b b = 0$. We obtain

$$\sum_{b \in B_1} \beta_b b + \sum_{b \in B_0} r_b b = 0$$

   Now use the linear independence of B (notice that $r_b b \in \mathbb{F}b$ for every $b \in B_0$) to conclude that every β_b is zero and that $r_b b = 0$ for every $b \in B_0$.

So we proved that every $r_b = 0$ if $b \in B_1$ and $r_b b = 0$ for every $b \in B$.

6. (Finite groups of exponent 2)

a) Describe representations of the group $\mathbb{Z}_2 \times \mathbb{Z}_2$ over a field $\mathbb{F}$ whose characteristic is not 2

b) Try to understand the category $\mathrm{Rep}_{\mathbb{F}}(G)$ where $\mathbb{F}$ and G are as in part a).

c) A group G has exponent 2 if $g^2 = 1$ for every $g \in G$. Find all finite groups of exponent 2 up to isomorphism.

d) Try to generalize a) and b) to get an idea of representations of finite groups of exponent 2 over fields of characteristic different from 2.

Solution:

a) Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(1,0),(0,1),(1,1)\}$, $H = \{(0,0),(1,0)\} \simeq \mathbb{Z}_2$. Assume $\varphi\colon G \to \mathrm{Aut}_{\mathbb{F}}(V)$. Our approach is based on these observations

(1) $\varphi' := \varphi|_H\colon H \to \mathrm{Aut}_{\mathbb{F}}(V)$ is a representation of H over $\mathbb{F}$.

(2) $\varphi((0,1)) \in \mathrm{Aut}_{\mathbb{F}}(V)$ is compatible with the action of H on V. In other words $\varphi((0,1)) \in \mathrm{Rep}_{\mathbb{F}}(\varphi', \varphi')$.

The first one is obvious. Let us check the second one: We have to prove $\forall h \in H$

$$\varphi((0,1)) \circ \varphi(h) = \varphi(h) \circ \varphi((0,1))\,.$$

Since φ is a representation, we have $\varphi((0,1)) \circ \varphi(h) = \varphi((0,1)+h)$ and $\varphi(h) \circ (\varphi(0,1)) = \varphi(h + (0,1))$ and $\varphi((0,1)) \circ \varphi(h) = \varphi(h) \circ \varphi((0,1))$ holds (even for every $h \in G$).

Now we use what we know about $\mathrm{Rep}_{\mathbb{F}}(H)$ from the lecture:

(1)' Let $V_+ := \{v \in V \mid [\varphi((1,0))](v) = v\}$ and $V_- = \{v \in V \mid [\varphi((1,0))](v) = -v\}$. Then $V = V_+ \oplus V_-$.

(2)' $[\varphi(0,1)](V_+) \subseteq V_+$ and $[\varphi(0,1)](V_-) \subseteq V_-$.

Since $\varphi(0,1)^2 = 1_V$, we have that $\varphi(0,1)|_{V_+} \in \mathrm{Aut}_{\mathbb{F}}(V_+)$ and $\varphi(0,1)|_{V_-} \in \mathrm{Aut}_{\mathbb{F}}(V_-)$.

Let $K = \{(0,0),(0,1)\}$. The representation φ induces two represenations of K over $\mathbb{F}$:

$$\varphi_+\colon K \to \mathrm{Aut}_{\mathbb{F}}(V_+); (0,0) \mapsto 1_{V_+}, (0,1) \mapsto \varphi((0,1))|_{V_+}$$

$$\varphi_-\colon K \to \mathrm{Aut}_{\mathbb{F}}(V_-); (0,0) \mapsto 1_{V_-}, (0,1) \mapsto \varphi((0,1))|_{V_-}$$

Apply our knowledge on representations of $\mathbb{Z}_2$ over $\mathbb{F}$ again: $V_+ = V_{++} \oplus V_{+-}$ $V_- = V_{-+} \oplus V_{--}$, where

$$V_{++} = \{v \in V_+ \mid [\varphi(0,1)](v) = v\}$$

$$V_{+-} = \{v \in V_+ \mid [\varphi(0,1)](v) = -v\}$$

$$V_{-+} = \{v \in V_- \mid [\varphi(0,1)](v) = v\}$$

$$V_{--} = \{v \in V_- \mid [\varphi(0,1)](v) = -v\}$$

Since $\varphi((1,1)) = \varphi((1,0)) \circ \varphi((0,1))$, the representation φ is determined by the values $\varphi((1,0))$ and $\varphi((0,1))$. These values are given by the decomposition of the space $V = V_{++} \oplus V_{+-} \oplus V_{-+} \oplus V_{--}$.

The following table summarizes our observations about φ

	V_{++}	V_{+-}	V_{-+}	V_{--}
$(0,0)$	$1_{V_{++}}$	$1_{V_{+-}}$	$1_{V_{-+}}$	$1_{V_{--}}$
$(1,0)$	$1_{V_{++}}$	$1_{V_{+-}}$	$-1_{V_{-+}}$	$-1_{V_{--}}$
$(0,1)$	$1_{V_{++}}$	$-1_{V_{+-}}$	$1_{V_{-+}}$	$-1_{V_{--}}$
$(1,1)$	$1_{V_{++}}$	$-1_{V_{+-}}$	$-1_{V_{-+}}$	$1_{V_{--}}$

(there are 4 φ-invariant subspaces and the table describes how elements of G act on these subspaces)

Conversely, let V_1, V_2, V_3, V_4 be $\mathbb{F}$-spaces and let $V = V_1 \oplus V_2 \oplus V_3 \oplus V_4$. Consider the following map $\varphi\colon G \to \mathrm{Aut}_{\mathbb{F}}(V)$

$$\varphi((0,0))\colon (v_1, v_2, v_3, v_4) \mapsto (v_1, v_2, v_3, v_4)$$

$$\varphi((1,0))\colon (v_1, v_2, v_3, v_4) \mapsto (v_1, v_2, -v_3, -v_4)$$

$$\varphi((0,1))\colon (v_1, v_2, v_3, v_4) \mapsto (v_1, -v_2, v_3, -v_4)$$

$$\varphi((1,1))\colon (v_1, v_2, v_3, v_4) \mapsto (v_1, -v_2, -v_3, v_4)$$

We want to check that φ is a homomorphism of groups. We easily verify that $\varphi((0,0)) = 1_V$, $\varphi(g)^2 = 1_V$ for every $g \in G$ and $\varphi(x) \circ \varphi(y) = \varphi(z)$ if $\{x, y, z\}$ is the set of all nonzero elements of G. From this it follows that $\varphi\colon G \to \mathrm{Aut}_{\mathbb{F}}(V)$ is a homomorphism of groups.

b) Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, $\varphi\colon G \to \mathrm{Aut}_{\mathbb{F}}(V)$ and $\varphi'\colon G \to \mathrm{Aut}_{\mathbb{F}}(V')$ two representations of G over $\mathbb{F}$, where $\mathrm{char}(\mathbb{F}) \neq 2$. We want to understand $\mathrm{Rep}_{\mathbb{F}}(G)(\varphi, \varphi')$. Keeping the notation from part a) we decompose $V = V_{++} \oplus V_{+-} \oplus V_{-+} \oplus V_{--}$ and $V' = V'_{++} \oplus V'_{+-} \oplus V'_{-+} \oplus V'_{--}$ according the action of $(1,0)$ and $(0,1)$ on V and V'.

First let us check that every $\theta \in \mathrm{Hom}_{\mathbb{F}}(V, V')$ preserving these decompositions is in $\mathrm{Rep}_{\mathbb{F}}(G)(\varphi, \varphi')$. That is assume that $\theta(V_{*,@}) \subseteq V_{*,@}$ for every $*, @ \in \{+,-\}$. We want to prove $\theta \circ [\varphi(g)] = [\varphi(g)] \circ \theta$ for every $g \in G$.

Let $v = v_{++} + v_{+-} + v_{-+} + v_{--}$, where $v_{++} \in V_{++}, v_{+-} \in V_{+-}, v_{-+} \in V_{-+}, v_{--} \in V_{--}$. Then

$$\theta([\varphi((1,0))](v)) = \theta(v_{++} + v_{+-} - v_{-+} - v_{--}) = \theta(v_{++}) + \theta(v_{+-}) - \theta(v_{-+}) - \theta(v_{--})$$

$$[\varphi'((1,0))]\theta(v) = [\varphi'((1,0))]\theta(v_{++} + v_{+-} + v_{-+} + v_{--}) =$$

$$[\varphi'((1,0))](\theta(v_{++}) + \theta(v_{+-}) + \theta(v_{-+}) + \theta(v_{--})) =$$

$$[\varphi'((1,0))](\theta(v_{++})) + [\varphi'((1,0))](\theta(v_{+-})) + [\varphi'((1,0))](\theta(v_{-+})) + [\varphi'((1,0))](\theta(v_{--})) =$$

$$\theta(v_{++}) + \theta(v_{+-}) - \theta(v_{-+}) - \theta(v_{--}).$$

(the last equality needs that θ preserves decompositions of V and V') We proved $[\varphi'((1,0))]\circ\theta = \theta\circ[\varphi((1,0))]$.

Similarly we proceed with other elements of G.

$$\theta([\varphi((0,1))](v)) = \theta(v_{++}-v_{+-}+v_{-+}-v_{--}) = \theta(v_{++})-\theta(v_{+-})+\theta(v_{-+})-\theta(v_{--})$$

$$[\varphi'((0,1))]\theta(v) = [\varphi'((0,1))]\theta(v_{++}+v_{+-}+v_{-+}+v_{--}) =$$

$$[\varphi'((0,1))](\theta(v_{++})+\theta(v_{+-})+\theta(v_{-+})+\theta(v_{--})) =$$

$$[\varphi'((0,1))](\theta(v_{++}))+[\varphi'((0,1))](\theta(v_{+-}))+[\varphi'((0,1))](\theta(v_{-+}))+[\varphi'(0,1)](\theta(v_{--})) =$$

$$\theta(v_{++})-\theta(v_{+-})+\theta(v_{-+})-\theta(v_{--})\,.$$

Thus we proved $[\varphi'((0,1))]\circ\theta = \theta\circ[\varphi((0,1))]$.

We could do the same for elements $(0,0)$ and $(1,1)$ but it is not necessary. In fact, $\varphi((0,0)) = 1_V$ and $\varphi'((0,0)) = 1_{V'}$ so $\theta\circ\varphi((0,0)) = \varphi'((0,0))\circ\theta$ holds for every $\theta\in\mathrm{Hom}_{\mathbb{F}}(V,V')$.

Since $(1,1) = (1,0)+(0,1)$ and we know $\theta\circ\varphi((1,0)) = \varphi'((1,0))\circ\theta$ and $\theta\circ\varphi((0,1)) = \varphi'((0,1))\circ\theta$ we get

$$\varphi'((1,1))\theta = \varphi'((1,0))\varphi'((0,1))\theta =$$

$$\varphi'((1,0))\theta\varphi((0,1)) = \theta[\varphi((1,0))\varphi((0,1))] = \theta\varphi((1,1))$$

Thus we proved that every linear map preserving decompositions of spaces is a homomorphism between the corresponding representations.

Conversely we can prove that every $\theta\in\mathrm{Rep}_{\mathbb{F}}(G)(\varphi,\varphi')$ preserves the decomposition. For example assume $v\in V_{++}$. Then

$$[\varphi'((1,0))](\theta(v)) = \theta([\varphi(1,0)](v)) = \theta(v),\ [\varphi'((0,1))](\theta(v)) = \theta([\varphi(0,1)](v)) = \theta(v)\,,$$

so $\theta(v)\in V_{++}$. Similarly if $v\in V_{+-}$

$$[\varphi'((1,0))](\theta(v)) = \theta([\varphi(1,0)](v)) = \theta(v),\ [\varphi'((0,1))](\theta(v)) = \theta([\varphi(0,1)](v)) = -\theta(v)\,,$$

so $\theta(v)\in V_{+-}$. If $v\in V_{-+}$,

$$[\varphi'((1,0))](\theta(v)) = \theta([\varphi(1,0)](v)) = -\theta(v),\ [\varphi'((0,1))](\theta(v)) = \theta([\varphi(0,1)](v)) = \theta(v)$$

so $\theta(v)\in V_{-+}$. And finally if $v\in V_{--}$, then

$$[\varphi'((1,0))](\theta(v)) = \theta([\varphi(1,0)](v)) = -\theta(v),\ [\varphi'((0,1))](\theta(v)) = \theta([\varphi(0,1)](v)) = -\theta(v)$$

so $\theta(v)\in V_{--}$.

Our conclusion is that a linear map $\theta\colon V\to V'$ is in $\mathrm{Rep}(\varphi,\varphi')$ if and only if $\theta(V_{++})\subseteq V'_{++}$, $\theta(V_{+-})\subseteq V'_{+-}$, $\theta(V_{-+})\subseteq V'_{-+}$ and $\theta(V_{--})\subseteq V'_{--}$.

The corresponding statment about the category of representations of G over $\mathbb{F}$ could be $\mathrm{Rep}_{\mathbb{F}}(G)\simeq\mathbb{F}{-}\mathrm{Mod}\times\mathbb{F}{-}\mathrm{Mod}\times\mathbb{F}{-}\mathrm{Mod}\times\mathbb{F}{-}\mathrm{Mod}$, where $\mathbb{F}$-Mod is the category of $\mathbb{F}$-spaces and linear maps.

c) Assume $g^2 = 1$ (or equivalenty $g = g^{-1}$) for every $g \in G$. Then G is commutative. Indeed, if $x, y \in G$, then

$$1 = (xy)(xy) \Rightarrow xy = y^{-1}x^{-1} = yx\,.$$

We can use a structure theorem for finite abelian groups: Every finite group is isomorphic to a product of cyclic groups. The only non-trivial cyclic group of exponent two is (up to an isomorphism) $\mathbb{Z}_2$. This shows that G has to be isomorphic to $\mathbb{Z}_2^k$ for some $k \in \mathbb{N}_0$.

d) We just sketch one of the possible ways how to proceed. Let $G = \mathbb{Z}_2^n$ and $e_1 = (1, 0, \dots, 0), e_2 = (0, 1, 0, \dots, 0), \dots, e_n = (0, \dots, 0, 1)$ be its canonical generators. The natural conjecture is that a representation $\varphi\colon G \to \mathrm{Aut}_{\mathbb{F}}(V)$ is described by a direct sum decomposition of φ into 2^n invariant subspaces (though some of them could be zero) and these spaces are determined by the action of canonical generators.

Let us try to describe it: Let $\Sigma := \{+, -\}^n$ (all ordered n-tuples of signs). For $\sigma \in \Sigma$ let V_σ be the set of all $v \in V$ such that $[\varphi(e_i)](v) = \pm v$ for each i, where the sign is determined by the i-th component of σ. We would expect $V = \oplus_{\sigma \in \Sigma} V_\sigma$.

We can prove this by induction (note we did the case $n = 1$ in the first lecture and the case $n = 2$ is the part a)). Let $H = \langle e_1, e_2 \dots, e_{n-1}\rangle$ and $K = \langle e_n \rangle$, that is, $H \simeq \mathbb{Z}_2^{n-1}$ and $K \simeq \mathbb{Z}_2$.

Consider $\varphi'\colon H \to \mathrm{Aut}_{\mathbb{F}}(V)$ and apply the induction hypothesis to get a decomposition of V into 2^{n-1} φ'-invariant spaces determined by the action of $e_1, \dots, e_{n-1}$. Let W be any of these φ'-invariant subspaces. Use the commutativity of G to show that $[\varphi(e_n)](W) \subseteq W$ and in fact $\varphi(e_n)|_W \in \mathrm{Aut}_{\mathbb{F}}(W)$.

We can consider a representation $\varphi_n\colon K \to \mathrm{Aut}_{\mathbb{F}}(W)$ and split W as $W = W_+ \oplus W_-$.

Doing this with every of the 2^{n-1} φ'-invariant subspaces given from the induction, we obtain 2^n φ-invariant spaces decomposing V.

Conversely, take 2^n vector spaces over $\mathbb{F}$. On each of this vector spaces define an action of G saying whether e_i acts on the space as the identity or the minus identity. Verify that you defined correctly a representation of G on each of these spaces. Then direct sum of these 2^n representations of G is again a representation of G. In the previous paragraph we showed how to prove that every representation of G over $\mathbb{F}$ is equivalent to a representation of G over $\mathbb{F}$ constructed in this way.