Groups and Vector Spaces: Strategy Guide.

January 16, 2020

I've taken a look at papers from 2017, 2018, and 2019 and looked for patterns and general strategies for questions.

1 Question 1:

The first quesion over the 3 available exam has been to determine whether or not a list of sets are groups. So a relevant definition is:

1.1 Definition. A *group* is a non-empty set G on which is defined an associative binary operation $\circ$ such that there is an identity e ($e \circ x = x$ and $x \circ e = x$ for all $x \in G$), and each $x \in G$ has an inverse in G (an element y such that $x \circ y = e$ and $y \circ x = e$).

The next question is then variable, usually it has something to do with a structural property of a group or subgroups, so a useful defintion to know here is:

1.2 Definition. Let $(G, \circ)$ be a group. A *subgroup* of $(G, \circ)$ is a subset H of G such that H becomes a group with the same operation $\circ$.

1.3 Lemma. *If H is a subgroup of G, then (i) they have the same identity element (in particular H contains the identity of G), and (ii) the inverse of any element of H is the same whether you use the group structure of H or that of G.*

1.4 Theorem (Subgroup criterion)**.** *Let $(G, \circ)$ be a group. A subset H of G is a subgroup if and only if it satisfies the following properties (i) $1 \in H$, (ii) $xy \in H$ for all $x, y \in H$, and (iii) $x^{-1} \in H$ for all $x \in H$.*

Proof. First suppose that (i), (ii) and (iii) hold. Then (ii) says that H is closed under $\circ$, and it inherits associativity from G. Then $1 \in H$ by (i), and it is an identity for H. Also each element $x \in H$ has an inverse in $x^{-1} \in H$ by (iii). Thus H is a subgroup.

Conversely suppose that H is a subgroup. Then since H is closed under $\circ$, (ii) holds. Now (i) and (iii) follow from the lemma. $\square$

There is also a high chance that in this question, or another, you may have to draw up a Cayley/Group table. We've also called these *Latin Squares.* The process for these is fairly simple, Let G be our group with elements $\{1, a, b \dots z\}$ and operation $\circ$, we construct the table thus:

$\circ$	1	a	b	$\dots$	z
1	1	a	b	$\vdots$	z
a	a	$a \circ a$	$b \circ a$	$\vdots$	$z \circ a$
b	b	$a \circ b$	$b \circ b$	$\vdots$	$z \circ b$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
z	z	$a \circ z$	$b \circ b$	$\vdots$	$z \circ z$

If G is *Abelian* then the table is symmetric about the diagonal. Relevant definition:

1.5 Definition. We say that a group $(G, \circ)$ is *abelian* if the operation $\circ$ is commutative, that is, $x \circ y = y \circ x$ for all $x, y \in G$.

Terms that come up that you may have forgotten:

- **Non-Singular Matrix**: A square matrix that is invertible, an invertible matrix has a non-zero determinant.

- **Coprime**: Two numbers x, y are coprime if and only if they share no prime factors.

2 Question 2:

Lagrange's Theorem has come up in 2/3 of the exams available to us here. While I haven't included the proof here (See the revision doc I made, Theorem 2.20) I will include the statement:

2.1 Theorem. *(Lagrange): If H is a subgroup of the finite group G, then $|H|$ divides $|G|$.*

In general this question is on structure of groups. So a set of useful definitions here are:

2.2 Definition. The *order* of a group G, denoted by $|G|$, is the number of elements in the set G, either a positive integer or infinity.

2.3 Definition. The *order* of an element x of a group G is the smallest integer $n > 0$ such that $x^n = 1$. If no such n exists we say that x has infinite order. (In an additive group the condition is $nx = 0$.)

2.4 Definition. If x is an element of a group G we let

$$\langle x \rangle = \{x^n : n \in \mathbb{Z}\}.$$

(or in additive notation $\langle x \rangle = \{nx : n \in \mathbb{Z}\}$). It is a subgroup of G. We call it the *subgroup of G generated by x*. We say that G is *generated by x*, or that x is a *generator* for G if $G = \langle x \rangle$. We say that G is a *cyclic* group if it has a generator.

2.5 Definition. If G and H are groups, then we consider the cartesian product

$$G \times H = \{(g, h) : g \in G, h \in H\}$$

with the operation $\circ$ defined by

$$(g, h) \circ (g', h') = (gg', hh').$$

It is easy to see that it is a group. We call it the *direct product* of G and H. The identity element is $1 = (1_G, 1_H)$. The inverse of (g, h) is (g^{-1}, h^{-1}). (If G and H are additive groups we use the notation $(g, h) + (g', h') = (g + g', h + h')$.)

2.6 Definition. Let $(G, \circ)$ and $(H, \circ)$ be groups. A mapping $\theta : G \to H$ is a *homomorphism* if $\theta(g \circ g') = \theta(g) \circ \theta(g')$ for all $g, g' \in G$. It is an *isomorphism* if in addition it is a bijection. We say that groups G and H are *isomorphic*, and write $G \cong H$, if there is an isomorphism $\theta : G \to H$.

2.7 Definition. The *kernel* of a homomorphism $\theta : G \to H$ is the set $\ker\theta = \{g \in G : \theta(g) = 1\}$. It is a subset of G. The *image* of a homomorphism $\theta : G \to H$ is the set $\operatorname{im}\theta = \{\theta(g) : g \in G\}$. It is a subset of H.

2.8 Theorem (First isomorphism theorem)**.** *If $\theta : G \to G'$ is a homomorphism, then there is an isomorphism $\overline{\theta} : G/\ker\theta \to \operatorname{im}\theta$ defined by $\overline{\theta}(Hg) = \theta(g)$, where $H = \ker\theta$.*

Proof. The map $\overline{\theta}$ is well-defined and injective since $Hx = Hy \Leftrightarrow xy^{-1} \in H = \ker\theta \Leftrightarrow \theta(xy^{-1}) = 1 \Leftrightarrow \theta(x)\theta(y)^{-1} = 1 \Leftrightarrow \theta(x) = \theta(y)$. It is clearly surjective, and it is a homomorphism by the definition of the product in G/H. $\square$

2.9 Definition. Let H be a subgroup of a group G. A *(right) coset* of H in G is a subset of the form

$$Hx = \{hx : h \in H\}$$

for some $x \in G$. If G is an additive group we use the notation $H + x = \{h + x : h \in H\}$ instead. Note that even if G is infinite, we still have the notion of 'right coset'. Finiteness is just used in the final part of the proof of Lagrange's Theorem.

2.10 Definition. Elements x, y of a group G are said to be *conjugate* in G if there is $g \in G$ with $y = g^{-1}xg$. The set of all elements conjugate to a given element x is called a *conjugacy class*. The conjugacy class containing x is

$$\operatorname{conj}_G(x) = \{g^{-1}xg : g \in G\}.$$

2.11 Definition. A subgroup H of a group G is said to be *normal* if $g^{-1}hg \in H$ for all $h \in H$ and $g \in G$. It is equivalent that H is a union of conjugacy classes. We denote this by $H \lhd G$.

Terms that come up that you may have forgotten:

- **Equivalence Relation**: A relation $x \sim y$ is an equivalence relations if and only if:

$$x \sim x \text{ (REFLEXIVITY)}$$
$$x \sim y \implies y \sim x \text{ (SYMMETRY)}$$
$$x \sim y, y \sim z \implies x \sim z \text{ (TRANSITIVITY)}$$

3 Question 3:

This question is on permutations in all available papers. So, relevant definition:

3.1 Definition. A *permutation* of a set A is a bijective mapping from A to itself, $\pi : A \to A$. The set of all permutations of A forms a group under composition of mappings $\pi \circ \sigma$, where

$$(\pi \circ \sigma)(a) = \pi(\sigma(a))$$

for $a \in A$. The identity element is the identity map *id*. Since π is bijective, it has an inverse mapping π^{-1}, and that is the inverse to π in this group. We shall only be interested in permutations of the set $A = \{1, 2, \ldots, n\}$ for n a positive integer. The set of all such permutations is called the *symmetric group of degree* n and denoted by S_n.

3.2 Definition. Let k, n be a positive integers with $k \leq n$ and let $a_1, a_2, \ldots, a_k$ be distinct elements in the set $\{1, 2, \ldots, n\}$. We denote by $(a_1\ a_2\ \ldots\ a_k)$ the permutation in S_n sending

$$a_1 \mapsto a_2 \mapsto a_3 \mapsto \cdots \mapsto a_k \mapsto a_1$$

and with $a \mapsto a$ for all a not in the list. It is called a *cycle of length* k or a k*-cycle*. A 2-cycle is also called a *transposition*.

3.3 Definition. The *sign* or *signature* of a permutation π is $\epsilon(\pi) = \det(A_\pi)$.

3.4 Definition. A permutation which can be written as a product of an odd/even number of transpositions is called an *odd/even permutation*.

3.5 Definition. The set of even permutations in S_n (which forms a subgroup of S_n) is called the *alternating group* A_n *of degree* n.

There are 2 types of notation here. One is *Cycle Notation* as defined above, then there is the table notation:

$$\begin{pmatrix} a_1 & a_2 & \ldots & a_k \\ \pi(a_1) & \pi(a_2 & \ldots & \pi(a_k) \end{pmatrix}$$

In table notation, finding the inverse and composition of 2 permutations is much easier. For example let:

$$G = \{1, 2, 3, 4\}$$
$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

To find the inverse of either, simply flip the table:

$$\pi^{-1} = \begin{pmatrix} 3 & 4 & 1 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$
$$\sigma^{-1} = \begin{pmatrix} 2 & 4 & 1 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

And you can then stack them to easily read off compositions:

$$\pi \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \\ 4 & 2 & 3 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$$
$$\sigma \circ \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

3.6 Remarks. (i) Cycle notation doesn't tell you which S_n you are working in. For example the cycle $(2\ 5\ 4)$ could be a permutation in S_n for any $n \geq 5$. (ii) A k-cycle can be written in k different ways. For example $(2\ 5\ 4) = (5\ 4\ 2) = (4\ 2\ 5)$. A 1-cycle is the identity. (iii) A k-cycle has order k. (iv) We say a collection if cycles is *disjoint* if there is no number a occurring in two of them. For example $(2\ 5\ 4)$ and $(1\ 3)$ are disjoint. Disjoint cycles commute, $(2\ 5\ 4)(1\ 3) = (1\ 3)(2\ 5\ 4)$.

3.7 Theorem. *Every permutation can be written as a product of disjoint cycles. The decomposition is essentially unique, apart from the order of the cycles and the different ways of writing a cycle.*

3.8 Corollary. *To find the order of a permutation, write it as a product of disjoint cycles and take the least common multiple of their lengths.*

4 Questions 4&5:

These questions are about vector spaces and linear mappings:

4.1 Definition. A *field* consists of a set F with binary operations $+$ and $\cdot$ satisfying (i) The operation $+$ turns F into an additive group. The identity element is denoted by 0. (ii) The product $a \cdot b$ is defined and in F for all $a, b \in F$, it is associative and commutative, and it turns $F^* = \{x \in F : x \neq 0\}$ into an abelian group. (iii) The product $\cdot$ is distributive over $+$, that is, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

4.2 Definition. Let F be a field. A *vector space over* F, or *an* F*-vector space* consists of a set V, whose elements are called *vectors*, together with operations of addition of vectors, $+$, and scalar multiplication satisfying the following axioms. (addition) The set V of vectors is an additive group under $+$. (closure) Scalar multiplication $a\mathbf{v}$ is defined and in V for all scalars $a \in F$ and $\mathbf{v} \in V$. (compatibility of multiplication) $(ab)\mathbf{v} = a(b\mathbf{v})$ for all $a, b \in F$ and $\mathbf{v} \in V$. (identity) $1\mathbf{v} = \mathbf{v}$ for all $\mathbf{v} \in V$. (distributivity) $a(\mathbf{v} + \mathbf{w}) = (a\mathbf{v}) + (a\mathbf{w})$ for all $a \in F$ and $\mathbf{v}, \mathbf{w} \in V$. $(a + b)\mathbf{v} = (a\mathbf{v}) + (b\mathbf{v})$ for all $a + b \in F$ and $\mathbf{v} \in V$. We denote by $\mathbf{0}$ the identity element for V under $+$. The zero vector. We can define subtraction for vectors by defining $\mathbf{u} - \mathbf{v}$ to be equal to $\mathbf{u} + (-\mathbf{v})$.

4.3 Definition. Let V be a vector space over a field F. By a *subspace* of V we mean a subset U of V such that U becomes a vector space with the same operations of addition of vectors and scalar multiplication in V.

4.4 Definition. Let V, W be vector spaces over a field F. A mapping $\theta : V \to W$ is called a *linear mapping* (or *linear transformation*, *linear operator*, or *homomorphism of vector spaces*) if (i) $\theta(\mathbf{v} + \mathbf{v}') = \theta(\mathbf{v}) + \theta(\mathbf{v}')$ for all $\mathbf{v}, \mathbf{v}' \in V$, and (ii) $\theta(a\mathbf{v}) = a\theta(\mathbf{v})$ for all $a \in F$ and $\mathbf{v} \in V$. (It follows that $\theta(a\mathbf{v} + b\mathbf{v}') = a\theta(\mathbf{v}) + b\theta(\mathbf{v}')$ for all $a, b \in F$ and $\mathbf{v}, \mathbf{v}' \in V$. In fact this can be used as a characterization of linear mappings.) An *isomorphism of vector spaces* is a linear map which is a bijection. If so, we write $V \cong W$.

4.5 Definition. The *span* of a finite set of vectors $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ in a vector space V is the set of all linear combinations of them,

$$\operatorname{span} S = \{a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n : a_1, \ldots, a_n \in F\}.$$

4.6 Definition. Let V be a vector space and let $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ be a finite subset of V. We say that S is *linearly independent* if there is no linear relation between the elements of S of the form

$$a_1\mathbf{v}_1 + \ldots + a_n\mathbf{v}_n = \mathbf{0}$$

with $a_1, \ldots, a_n \in F$, other than the trivial one with $a_1 = \ldots = a_n = 0$. Otherwise S is said to be *linearly dependent*.

4.7 Definition. Let V be a vector space. We say that a finite set of vectors $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is a *basis* of V if it is linearly independent and it spans V (i.e. $\operatorname{span} S = V$).

4.8 Definition. Let V be a vector space over F. If U is a subspace of V, then the *quotient vector space* V/U is the quotient group under addition, with scalar multiplication defined by $a(U+\mathbf{v}) = U + a\mathbf{v}$. It is easy to see that the natural map $V \to V/U$, $\mathbf{v} \mapsto U + \mathbf{v}$ is a linear map.

4.9 Definition. If $\theta : V \to W$ is a linear map, then the *rank* of θ is $r(\theta) = \dim \operatorname{im} \theta$ and the *nullity* of θ is $n(\theta) = \dim \ker \theta$.

4.10 Definition. Suppose that $S = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ is a basis of a vector space V over F. In this case the map $\phi_S : F^n \to V$ is an isomorphism. Thus for each $\mathbf{v} \in V$ there is a unique vector $\mathbf{x} = (x_1, \dots, x_n)^T \in F^n$ such that $\mathbf{v} = x_1\mathbf{v}_1 + \cdots + x_n\mathbf{v}_n$. We call it the *coordinates of* $\mathbf{v}$ *with respect to* S, and denote it by $[\mathbf{v}]_S$.

4.11 Theorem (Subspace criterion)**.** *Let V be a vector space over a field F. A subset U of V is a subspace if and only if it satisfies the following properties (i) $\mathbf{0} \in U$. (ii) For all $\mathbf{u}, \mathbf{u}' \in U$ we have $\mathbf{u} + \mathbf{u}' \in U$, and (iii) For all scalars $a \in F$ and elements $\mathbf{u} \in U$ we have $a\mathbf{u} \in U$.*

Then we have all the matrix related theorems (These usually come up in Q5 but are relevant to before)

4.12 Definition. Let $\theta : V \to W$ be a linear map, let $S = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ be a basis of V and let $R = \{\mathbf{w}_1, \dots, \mathbf{w}_m\}$ be a basis of W. The *matrix of θ with respect to the basis S of V and the basis T of W* is the matrix $A = (a_{ij})$ whose jth column is the coordinates of $\theta(\mathbf{v}_j)$ with respect to R.

Thus

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

where

$$\begin{aligned} \theta(\mathbf{v}_1) &= a_{11}\mathbf{w}_1 + a_{21}\mathbf{w}_2 + \cdots + a_{m1}\mathbf{w}_m \\ \theta(\mathbf{v}_2) &= a_{12}\mathbf{w}_1 + a_{22}\mathbf{w}_2 + \cdots + a_{m2}\mathbf{w}_m \\ \dots \\ \theta(\mathbf{v}_n) &= a_{1n}\mathbf{w}_1 + a_{2n}\mathbf{w}_2 + \cdots + a_{mn}\mathbf{w}_m. \end{aligned}$$

or $\theta(\mathbf{v}_j) = \sum_{i=1}^n a_{ij}\mathbf{w}_i$.

Special case. If $\theta : V \to V$ is a linear map from a vector space to itself, and we use the same basis for both the source and target copies of V, then we speak of the *matrix of θ with respect to S*.

4.13 Definition. If $S = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ and $S' = \{\mathbf{v}'_1, \dots, \mathbf{v}'_n\}$ are bases of V then the *transition matrix from S to S'* is the matrix $P = (p_{ij})$ whose jth column is the coordinates of $\mathbf{v}'_j$ with respect to S. Thus $\mathbf{v}'_j = \sum_{i=1}^n p_{ij}\mathbf{v}_i$.

We have $[\mathbf{v}]_S = P[\mathbf{v}]_{S'}$ for $\mathbf{v} \in V$ since if $\mathbf{x} = [\mathbf{v}]_{S'}$, then

$$\mathbf{v} = \sum_{j=1}^n x_j\mathbf{v}'_j = \sum_{j=1}^n x_j \sum_{i=1}^n p_{ij}\mathbf{v}_i = \sum_{i=1}^n (\sum_{j=1}^n p_{ij}x_j)\mathbf{v}_i = \sum_{i=1}^n (P\mathbf{x})_i\mathbf{v}_i.$$

Note that P is invertible; its inverse is the transition matrix in the opposite direction.

4.14 Definition. Two $n \times n$ matrices A, A' are *similar* if there is an invertible matrix P with $A' = P^{-1}AP$.

4.15 Definition. Suppose A is an $n \times n$ matrix and $\lambda \in F$.
Geometric multiplicity of λ = dimension of the λ-eigenspace $Esp(\lambda)$ for A.
Algebraic multiplicity of λ = multiplicity of λ as a root of the characteristic poly $\chi_A(t)$.

4.16 Definition. A set of vectors $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ is *orthogonal* if $\mathbf{v}_i \cdot \mathbf{v}_j = 0$ for all $i \neq j$. It is *orthonormal* if also $|\mathbf{v}_i| = 1$ for all i, so

$$\mathbf{v}_i \cdot \mathbf{v}_i = \begin{cases} 1 & (i = j) \\ 0 & (i \neq j). \end{cases}$$

4.17 Definition. A real $n \times n$ matrix P is said to be *orthogonal* if it is invertible and $P^{-1} = P^T$, that is, $P^TP = I = PP^T$.

(In fact you only need to check that $P^TP = I$. It follows that $\det P \neq 0$, so P is invertible, so $P^{-1} = P^T$.)

The set of orthogonal matrices forms a subgroup $O_n(\mathbb{R})$ of $\mathrm{GL}_n(\mathbb{R})$, the *orthogonal group*. The set of orthogonal matrices of determinant 1 forms a subgroup $SO_n(\mathbb{R})$, the *special orthogonal group*.

Terms that come up that you may have forgotten:

- **Eigenvalues**: Eigenvalues of a matrix A are given by the characteristic equation:

$$0 = |A - \lambda I|$$

  solved for λ. On a diagonalised matrix these can be read off the diagonal.

- **Eigenvectors**: An eigenvector $\mathbf{v}$ of a matrix A corresponds to an eigenvalue λ as such:

$$A\mathbf{v} = \lambda\mathbf{v}$$

  which are found using simultaneous equations. For a simple example we will take the 2x2 matrix:

$$\begin{aligned}
A &= \begin{pmatrix} 3 & 2 \\ 3 & -2 \end{pmatrix} \\
0 &= (3-\lambda)(-2-\lambda) - 6 \\
0 &= \lambda^2 - \lambda - 12 \\
\lambda_1 &= 4 \\
\lambda_2 &= -3 \\
\mathbf{v}_1 &= \begin{pmatrix} v_{11} \\ v_{12} \end{pmatrix} \\
\mathbf{v}_2 &= \begin{pmatrix} v_{21} \\ v_{22} \end{pmatrix} \\
\begin{pmatrix} 3 & 2 \\ 3 & -2 \end{pmatrix}\begin{pmatrix} v_{11} \\ v_{12} \end{pmatrix} &= 4\begin{pmatrix} v_{11} \\ v_{12} \end{pmatrix} \\
3v_{11} + 2v_{12} &= 4v_{11} \\
2v_{12} &= v_{11} \\
\mathbf{v}_1 &= \begin{pmatrix} 1 \\ 2 \end{pmatrix} \\
\begin{pmatrix} 3 & 2 \\ 3 & -2 \end{pmatrix}\begin{pmatrix} v_{21} \\ v_{22} \end{pmatrix} &= -3\begin{pmatrix} v_{21} \\ v_{22} \end{pmatrix} \\
3v_{21} + 2v_{22} &= -3v_{21} \\
2v_{22} &= -6v_{21} \\
v_{22} &= -3v_{21} \\
\mathbf{v}_2 &= \begin{pmatrix} 1 \\ -3 \end{pmatrix}
\end{aligned}$$

Note, these have not been *normalised*. To normalise a vector divide it by its length, so to normalise our above:

$$\begin{aligned}
\hat{\mathbf{v}_1} &= \frac{1}{\sqrt{5}}\begin{pmatrix} 1 \\ 2 \end{pmatrix} \\
\hat{\mathbf{v}_2} &= \frac{1}{\sqrt{10}}\begin{pmatrix} 1 \\ -3 \end{pmatrix}
\end{aligned}$$

A final note for this little summary. I have definitely cu a lot out here but this should *generally* get you through the past papers. Do not rely solely on this, look at examples/homeworks for additional practice and good luck!