Mat 247 - Definitions and results on group theory

Definition: Let $G$ be nonempty set together with a binary operation (usually called multiplication) that assigns to each pair of elements $g_1, g_2 \in G$ an element in $G$, denoted by $g_1g_2$ or $g_1 \cdot g_2$. We say that $G$ is a group under this operation if the following three properties are satisfied:

- Associativity: $(g_1g_2)g_3 = g_1(g_2g_3)$ for all $g_1, g_2, g_3 \in G$.
- Existence of identity element: There exists an element $e$ (called an identity) in $G$ such that $g \cdot e = e \cdot g = g$ for all $g \in G$.
- Existence of inverses: Let $e$ be an identity element in $G$. For each element $g \in G$, there is an element $g^{-1} \in G$ (called an inverse of $g$) such that $g \cdot g^{-1} = g^{-1} \cdot g = e$.

Examples: (details omitted)

1. If $F$ is a field and $n$ is a positive integer, let $GL_n(F) = \{ A \in M_{n \times n}(F) \mid \det(A) \neq 0 \}$. Then $GL_n(F)$ is a group under the operation of matrix multiplication.
2. Let $V$ be a finite-dimensional vector space over a field $F$. Let $G = \{ T \in L(V) \mid T$ is invertible $\}$. Then $GL(V)$ is a group under the operation of composition of linear transformations.
3. Let $n$ be a positive integer. The set $U_n$ of (complex) unitary $n \times n$ matrices is a group under the operation of matrix multiplication.
4. The set $\mathbb{Z}$ of integers is a group under the operation of addition of integers. (Note: $e = 0$; the inverse of $m \in \mathbb{Z}$ is $-m$.)
5. The set $\mathbb{Z}\{0\}$ of nonzero integers is not a group under the operation of multiplication of integers. The operation is associative and 1 is an identity, but the only nonzero integers that have inverses in $\mathbb{Z}\{0\}$ are 1 and $-1$.

Definition: If $G$ is a group, we say that $G$ is abelian (or commutative) if $g_1g_2 = g_2g_1$ for all $g_1$ and $g_2 \in G$. If $G$ is not abelian, we say that $G$ is nonabelian (or noncommutative).

Definition: The order of a group $G$ is the number of elements in $G$. If the order of $G$ is finite, we say that $G$ is a finite group. Otherwise, we say that $G$ is an infinite group.

If $G$ is an abelian group, the group operation may be written with a plus sign: $g_1 + g_2$ instead of $g_1g_2$.

Examples. If $F$ is a finite field, then $GL_n(F)$ is a finite group. If $F$ is an infinite field, then $GL_n(F)$ is an infinite group. If $n \geq 2$, then $GL_n(F)$ is a nonabelian group. The notation $F^\times$ is often used for the group $GL(1)$ of nonzero elements in $F$ (with the operation of multiplication in $F$). The group $F^\times$ is abelian.

Lemma. If $G$ is a group, there is a unique identity element in $G$. If $g \in G$, there is a unique inverse $g^{-1}$ of $g$ in $G$.

Proof. If $e$ and $e'$ are identity elements in $G$, we have $e \cdot e' = e' \cdot e = e$, using that $e'$ is an identity element, and we also have $e \cdot e' = e' \cdot e = e'$, since $e$ is an identity element. Therefore $e \cdot e' = e = e'$. The second part is left as an exercise.

Definition. If $H$ is a (nonempty) subset of a group $G$ and $H$ is itself a group under the operation on $G$, we say that $H$ is a subgroup of $G$.

The subset $\{e\}$ of a group $G$ is a subgroup of $G$. Clearly, $G$ is a subgroup of $G$. The proof of the following lemma was discussed in class.
**Examples:**

1. Let $G = \text{GL}_n(F)$, $n \geq 2$, and let $H = \{ A \in G \mid A_{jk} = 0 \text{ whenever } j > k \}$. Then $H$ is a subgroup of $G$. (Details omitted.)

2. Let $V$ be a vector space of dimension $n \geq 2$, let $G = \text{GL}(V)$, and let $H = \{ T \in G \mid \text{nullity}(T - I_V) > 0 \}$. Let $\beta = \{ x_1, \ldots, x_n \}$ be an ordered basis for $V$. There exists a unique $T \in \mathcal{L}(V)$ such that $T(x_1) = x_1$ and $T(x_j) = -x_j$, $2 \leq j \leq n$. Check that $T$ is invertible, $\text{nullity}(T - I_V) = 1$, $-T$ is invertible, and $\text{nullity}(-T - I_V) = n - 1$ (left as an exercise). This implies that $T, -T \in H$. Let $T \circ (-T)$ be identity elements in $H$. This implies that $H$ is not a subgroup of $G$.

3. Let $G = \text{GL}_n(F), n \geq 2$. Let $D_n$ be the set of diagonal matrices in $G$. Then $D_n$ is a subgroup of $G$, and $D_n$ is abelian. (This example shows that there can be nontrivial abelian subgroups of nonabelian groups.)

**Definition.** A subgroup $H$ of a group $G$ is said to be normal in $G$ if $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.

**Examples.** (details omitted)

1. Let $G = \text{GL}_2(F)$ and let $H = \{ A \in G \mid A_{21} = 0 \}$. Then $H$ is a subgroup of $G$ but $H$ is not normal in $G$. (Note that $h = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in H$, Let $g = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Show that $g \in G$ and $ghg^{-1} \notin H$.)

2. Let $G = \text{GL}_n(F), n \geq 2$, and let $H = \text{SL}_n(F) = \{ A \in G \mid \det(A) = 1 \}$. Then $H$ is a normal subgroup of $G$. (This is easily proved using properties of determinants.)

3. If $G$ is an abelian group, then any subgroup $H$ of $G$ is normal in $G$ because $ghg^{-1} = h(g \cdot g^{-1}) = h \cdot e = h$ for all $h \in H$ and $g \in G$.

**Definition.** If $G$ and $G'$ are groups, a map $\varphi : G \to G'$ is a homomorphism if $\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2)$ for all $g_1$ and $g_2 \in G$.

**Examples.** (details omitted)

1. Then $\det : \text{GL}_n(F) \to F^\times = \text{GL}_1(F)$ is a homomorphism.

2. If $G$ is a nonabelian group, the map $\varphi : G \to G$ defined by $\varphi(g) = g^2$ is not a homomorphism. (Here, $g^2 = g \cdot g$, $g \in G$.)

**Notation.** If $G$ is a group, $g \in G$, and $n \in \mathbb{Z}$, define $g^0 = e$, $g^n = g \cdot g^{n-1}$, $n \geq 1$, and $g^n = (g^{-1})^{-n}$, $n \leq -1$.

**Lemma.** Let $G$ and $G'$ be groups and let $\varphi : G \to G'$ be a homomorphism.

1. Let $e$ and $e'$ be identity elements in $G$ and $G'$, respectively. Then $\varphi(e) = e'$.

2. If $g \in G$ and $n \in \mathbb{Z}$, then $\varphi(g^n) = (\varphi(g))^n$.

**Definition:** Let $G$ and $G'$ be groups and let $\varphi : G \to G'$ be a homomorphism.

1. The kernel of $\varphi$ is defined to be $\{ g \in G \mid \varphi(g) = e' \}$. Here, $e'$ is the identity element in $G'$.

2. The image of $\varphi$ is defined to be $\varphi(G) = \{ \varphi(g) \mid g \in G \}$. 

2
Theorem. Let \( \varphi : G \rightarrow G' \) be a homomorphism. Then

1. The kernel of \( \varphi \) is a normal subgroup of \( G \).
2. \( \varphi \) is one-to-one if and only if the kernel of \( \varphi \) is equal to \( \{ e \} \).
3. The image \( \varphi(G) \) of \( \varphi \) is a subgroup of \( G' \).

Examples.

1. The kernel of \( \det : GL_n(F) \rightarrow F^\times \) is \( SL_n(F) \). Therefore \( SL_n(F) \) is a normal subgroup of \( GL_n(F) \).

2. The map \( \varphi : Z \rightarrow Z \) defined by \( \varphi(m) = 3m \) is a homomorphism. (Here, the operation on \( Z \) is addition of integers and we use additive notation for this operation.) The kernel of \( \varphi \) is equal to \( \{ e \} = \{ 0 \} \), so \( \varphi \) is one-to-one. Note that \( \varphi(Z) = \{ 3m \mid m \in Z \} \neq Z \).

Definition. Suppose that \( G \) is a group and \( g \in G \).

1. we say that \( g \) has finite order if \( g^n = e \) for some positive integer \( n \). In this case, the smallest positive integer such that \( g^n = e \) is called the order of \( g \).
2. If \( g^n \neq e \) for all positive integers \( n \), we say that \( g \) has infinite order.

Definition. Suppose that \( S \) is a nonempty subset of a group \( G \). The subgroup generated by \( S \), written \( \langle S \rangle \), is defined to be the smallest subgroup of \( G \) that contains the set \( S \). If \( \langle S \rangle = G \), we say that \( S \) is a set of generators for the group \( G \). If \( G = \langle g \rangle \) for some element \( g \in G \), we say that \( G \) is a cyclic group.

Lemma. If \( S \) is a subset of a group \( G \) and \( G = \langle S \rangle \), then \( G \) is abelian if and only if \( g_1g_2 = g_2g_1 \) for all \( g_1 \) and \( g_2 \in S \).

Examples.

1. If \( g \in G \) has order \( n \), then \( \langle g \rangle = \{ e, g, g^2, \ldots, g^{n-1} \} \).

2. Let \( G = GL_3(\mathbb{R}) \) and

\[
A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.
\]

The matrix \( A \) has order 3 because \( A^3 = I_n, A^2 \neq I_n \) and \( A \neq I_n \). The matrix \( B \) has infinite order because \( B^m \neq I_n \) for any positive integer \( m \).

3. If \( g \in G \) has infinite order, then

\( \langle g \rangle = \{ e, g, g^{-1}, g^2, g^{-2}, g^3, g^{-3}, \ldots, g^j, g^{-j}, \ldots \} \).

4. If \( G = \mathbb{Z} \), with group operation given by addition of integers, \( \langle 1 \rangle = \mathbb{Z} \), so \( \mathbb{Z} \) is an infinite cyclic group.

Lemma. Suppose that \( G \) is a group and \( g \in G \).

1. If \( n \) is a positive integer such that \( g^n = e \), then the order of \( g \) divides \( n \).
2. Suppose that the order of \( g \) is equal to \( n \). If \( m \geq 1 \), let \( \gcd(m, n) \) be the largest positive integer that divides both \( m \) and \( n \). Then the order of \( g^m \) is equal to \( n/\gcd(m, n) \).
Lemma. Suppose that $G$ and $G'$ are groups and $\varphi : G \to G'$ is a homomorphism.

1. If $G$ is abelian, then $\varphi(G)$ is abelian.
2. If $G$ is nonabelian and $\varphi(G)$ is abelian, then $\varphi$ is not one-to-one.
3. If $S = \{ g_1, \ldots, g_k \}$ is a set of generators for the group $G$, then $\varphi(S)$ is a set of generators for $\varphi(G)$. Furthermore, $\varphi(G)$ is abelian if and only if $\varphi(g_i g_j) = \varphi(g_j g_i)$ whenever $1 \leq i, j \leq k$ and $i \neq j$.
4. If $g \in G$ has finite order $n$, then the order of $\varphi(g)$ divides $n$.

Definition. A map $\varphi : G \to G'$ is said to be an isomorphism (of groups) if $\varphi$ is a homomorphism, $\varphi$ is one-to-one, and $\varphi$ is onto. In this case, we say that the groups $G$ and $G'$ are isomorphic.

Lemma. Let $G$ and $G'$ be groups. If $\varphi : G \to G'$ is an isomorphism, then the inverse function $\varphi^{-1} : G' \to G$ is an isomorphism of groups.

Examples: (details omitted)

1. If $G$ is abelian and $G'$ is nonabelian, then $G$ and $G'$ are not isomorphic.
2. Let $V$ be an $n$-dimensional vector space over a field $F$. Then $GL(V)$ and $GL_n(F)$ are isomorphic groups. Let $\beta$ be an ordered basis for $V$. Define $\varphi : GL(V) \to GL_n(F)$ by $\varphi(T) = [T]_\beta$. As explained in class, results from Mat 240 can be used to prove that $\varphi$ is a homomorphism and $\varphi$ is one-to-one and onto.
3. Let $G$ be a group. Fix an element $g \in G$. Define $\varphi(x) = gxg^{-1}$, $x \in G$. Then $\varphi$ is an isomorphism. Note that
   \[ \varphi(xy) = g(xy)g^{-1} = gx(g^{-1}g)yg^{-1} = (gxg^{-1})(gyg^{-1}) = \varphi(x)\varphi(y), \quad x, y \in G. \]
   This shows that $\varphi$ is a homomorphism. To see that $\varphi$ is an isomorphism, show that $x \mapsto g^{-1}xg$ is the inverse function.

Lagrange’s Theorem. Let $H$ be a subgroup of a finite group $G$. Then the order of $H$ divides the order of $G$.

If $g \in G$ has finite order, then the order of the subgroup $\langle g \rangle$ is equal to the order of the element $g$.

Corollary. If $G$ is a group of finite order and $g \in G$, then the order of $g$ divides the order of $G$.

Lemma. Let $T \in L(\mathbb{R}^3)$. Make $\mathbb{R}^3$ into an inner product space using the standard inner product. Assume that $T$ is orthogonal. Let $\beta$ be an orthonormal basis for $\mathbb{R}^3$. Let $A = [T]_\beta$.
   (Because $\beta$ is orthonormal and $T$ is orthogonal, we know that $A$ is an orthogonal matrix: $AA^t = A^tA = I_3$.)

1. If $\det(A) = 1$, then $1$ is an eigenvalue of $T$ and $T$ is a rotation.
2. If $\det(A) = -1$, then $T$ is the composition of a rotation and a reflection.
Dihedral groups

For each integer $n \geq 3$, let $D_n$ be the set of symmetries of a regular $n$-gon. A symmetry is obtained by taking a copy of the $n$-gon and then placing the copy back on the original $n$-gon so that it exactly covers it. We can describe the symmetries by first choosing a labelling of the $n$-vertices. We label the vertices consecutively from 1 to $n$, moving counterclockwise at the numbers increase. Each symmetry is determined uniquely by where it sends the vertices. For example, if $r$ is a rotation $2\pi/n$ radians clockwise about the centre of the $n$-gon, then $r$ moves vertex $i$ to the place where vertex $i+1$ was located before the $n$-gon was moved. For convenience, we place the $n$-gon in $\mathbb{R}^2$ so that the centre lies at the origin and reflection about the $x$-axis belongs to $D_n$. We denote this reflection by $s$. Relative to the standard basis $\beta = \{e_1, e_2\}$ for $\mathbb{R}^2$, $[s]_\beta = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. (Note that if we identify $\mathbb{R}^2$ with the subspace $\text{Span}\{e_1, e_2\}$ of $\mathbb{R}^3$, we find that $s$ is the restriction to $\text{Span}\{e_1, e_2\}$ of the rotation of $\mathbb{R}^3$ about the axis $\text{Span}\{e_1\}$—this rotation has matrix $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ relative to the basis $\{e_1, e_2, e_3\}$. This is an example of rotation of $\mathbb{R}^3$ that becomes a reflection upon restriction to a particular 2-dimensional invariant subspace.) We make $D_n$ into a group by defining $xy$ for $x, y \in D_n$ to be the symmetry obtained by first applying $y$ and then applying $x$ to the $n$-gon. The subgroup $\langle r \rangle = \{e, r, \ldots, r^{n-1}\}$ has order $n$, and $r^j$ is rotation counterclockwise about the centre through $2\pi j/n$ radians. The other elements in $D_n$ consist of reflections about axes of symmetry of the $n$-gon. If $n$ is even, there are $n/2$ axes of symmetry that pass through opposite vertices and $n/2$ axes of symmetry that perpendicularly bisect two opposite sides of the $n$-gon, giving a total of $n$ reflections. If $n$ is odd, each axis of symmetry passes through a vertex and the midpoint of the opposite side, giving a total of $n$ reflections. Thus $D_n$ has order $2n$. The following are some basic properties of $D_n$:

- $e, r, r^2, \ldots, r^{n-1}$ are distinct and $r^n = e$.
- $r^j s$ has order 2 for $1 \leq j \leq n$.
- $r s = s r^{-1}$. (Note that, since $r \neq r^{-1}$, this implies that $D_n$ is nonabelian.)
- $D_n = \langle r, s \rangle = \{e, r, \ldots, r^{n-1}, s, r s, r^2 s, \ldots, r^{n-1} s\}$.

**Lemma.** If $G$ is a group and $\varphi : D_n \rightarrow G$ is a function, then $\varphi$ is a homomorphism if $\varphi(r)^n = \varphi(s)^2 = e_G$, $\varphi(r^j) = (\varphi(r))^j$, and $\varphi(r s) = \varphi(r^j) \varphi(s) = \varphi(s) \varphi(r)^{-1} = \varphi(sr^{-j})$ for $1 \leq j \leq n - 1$. 

5