MAT 247S - Partial solutions to problem set 8

8. a) Let $\beta = \{ x_1, \ldots, x_n \}$ be a basis for V. Let T, U be linear operators on V such that $A = [T]_\beta$ is a diagonal matrix with $A_{11} = 1$ and $A_{jj} = -1$, $2 \leq j \leq n$, and $B = [U]_\beta$ is a diagonal matrix with entries $B_{jj} = 2$, $1 \leq j \leq n-1$ and $B_{nn} = 1$. Note that $x_1 \in N(T - 1_V)$ and $x_n \in N(U - 1_V)$. Also $\det A \neq 0$ and $\det B \neq 0$ imply that T, $U \in GL(V)$. Therefore T, $U \in H$. Now $C = [TU]_\beta$ is the diagonal matrix with $C_{11} = 2$, $C_{jj} = -2$ for $2 \leq j \leq n-1$, and $C_{nn} = -1$. The matrix $C - I = [TU - 1_V]_\beta$ has determinant equal to $(-1)^{n-1} 2^{n-1}$. Since $\det(C - I) \neq 0$, the operator $TU - 1_V$ is invertible and hence $N(TU - 1_V) = \{ 0 \}$. That is, $TU \notin H$. Since T, $U \in H$ and $TU \notin H$, H is not a subgroup of $GL(V)$.

8. b) Note that $I \in H$, so H is a nonempty set. Suppose that $A = \begin{pmatrix} a_1 & 3b_1 \\ b_1 & a_1 \end{pmatrix} \in H$ and $B = \begin{pmatrix} a_2 & 3b_2 \\ b_2 & a_2 \end{pmatrix} \in H$. Then $B^{-1} = (a_2^2 - 3b_2^2)^{-1} \begin{pmatrix} a_2 & -3b_2 \\ -b_2 & a_2 \end{pmatrix} \in H$ since $a_2/(a_2^2 - 3b_2^2)$ and $-b_2/(a_2^2 - 3b_2^2)$ are rational numbers. Calculating the product AB^{-1} (details omitted), we get $AB^{-1} = \begin{pmatrix} a' & 3b' \\ b' & a' \end{pmatrix}$, where $a' = (a_1 a_2 - 3b_2 b_2)/(a_2^2 - 3b_2^2)$ and $b' = (-a_1 b_2 - b_1 a_2)/(a_2^2 - 3b_2^2)$. Therefore $AB^{-1} \in H$ for all A, $B \in H$, and H is a subgroup of G.

8. c) Let $A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Check that $A^2 = B^2 = I$ but $(AB)^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 \neq I$. Therefore A, $B \in H$, but $AB \notin H$. Thus H is not a subgroup of $GL_2(F)$.

8. d) Note that $I \in H$, so H is nonempty. Check that if A, $B \in H$, then $AB^{-1} \in H$ (details omitted). It follows that H is a subgroup of G. Next, let $A \in H$ and $B \in G$. Check that since A and B are upper triangular invertible matrices, the matrix BAB^{-1} is an upper triangular invertible matrix. The characteristic polynomial of an upper triangular matrix C is equal to $(-1)^n (t - C_{11})(t - C_{22}) \cdots (t - C_{nn})$. Since A and BAB^{-1} are similar matrices, they must have the characteristic polynomial. Note that the characteristic polynomial of A is $(-1)^n (t-1)^n$. This is also the characteristic polynomial of BAB^{-1}. Since BAB^{-1} is upper triangular, it follows that every diagonal entry of BAB^{-1} is equal to 1. That is, $BAB^{-1} \in H$. We have shown that $BAB^{-1} \in H$ for every $A \in H$ and $B \in G$. Therefore H is a normal subgroup of G.

8. e) Because the inverse of an diagonal matrix is diagonal, and the product of two diagonal matrices is diagonal, H is a subgroup of G. Let $B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ and $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Note that $A \in H$ and $B \in G$, but $BAB^{-1} = \begin{pmatrix} 1 & -2 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ is not a diagonal matrix, so is not in H. Therefore H is not a normal subgroup of G.

8. f) Note that $I \in H$, so H is nonempty. Check that if A, $B \in H$, then $AB^{-1} \in H$ (details omitted). Let $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Note that $A \in H$ and $B \in G$, but $BAB^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \notin H$. Therefore H is not a normal subgroup of G.

9. Suppose that $x^2 = e$ for all $x \in G$. Then $x = x^{-1}$ for all $x \in G$. Let $x,\ y \in G$. We have $xyxy = e$. Multiply both sides by yx to get $xyxyyx = xyxex = xye = xy = yx$. Therefore G is abelian.

10. a) One part follows from the definition of subgroup. For the other, assume that H is nonempty, $H = \{\, x_1, \dots, x_n \,\}$ for some $x_1, \dots, x_n \in G$. Suppose that $x_i x_j \in H$ for $1 \le i,\ j \le n$. Note that $x_i x_1, \dots, x_i x_n \in H$. Suppose that $x_i x_j = x_i x_\ell$ for some i and ℓ. Multiplying on the left by x_i^{-1}, we get $x_j = x_\ell$. Therefore the subset $\{\, x_i x_1, \dots, x_i x_n \,\}$ of H contains exactly n elements, and must be equal to H. Since $x_i \in H$, we must have $x_i = x_i x_j$ for some j. Multiplying on the left by x_i^{-1}, we get $x_j = e$. Thus $e \in H$. Since $e \in H$, we have $e = x_i x_\ell$ for some ℓ. Multiplying on the left by x_i^{-1}, we get $x_\ell = x_i^{-1}$. Thus $x_i^{-1} \in H$. Finally, take $x_j,\ x_k \in H$. From what we just, did, we have $x_j^{-1} \in H$. By assumption H is closed under multiplication, so $x_k x_j^{-1} \in H$. This shows that $x_k x_j^{-1} \in H$ for all x_k and $x_j \in H$. That is, H is a subgroup of G (note that H was assumed to be nonempty).

10. b Let $G = \mathbb{Z}$ and let H be the set of positive integers. If m and $n \in H$, that is, $m > 0$ and $n > 0$, then $m + n > 0$. So H is closed under multiplication(note that the multiplication in G is just addition of integers). But H is not a subgroup of G, because inverses of elements in H don't belong to H (the inverse of n is $-n$ - if $n > 0$, then $-n < 0$, so $-n \notin H$).

11. Let $A \in U_n$. There exists $C \in GL_n(\mathbb{C})$ such that $C^{-1}AC = D$ is a diagonal matrix and every diagonal entry of D has absolute value one. Show that $(C^{-1}AC)^j = C^{-1}A^jC$ for every positive integer j. Use this to show that $(C^{-1}AC)^j = I$ if and only if $A^j = I$ (details omitted). This implies that A and $D = C^{-1}AC$ have the same order. Now let $\lambda_1, \dots, \lambda_n$ be the diagonal entries of D. Note that the D^j is a diagonal matrix, with diagonal entries $\lambda_1^j, \dots, \lambda_n^j$. Therefore $D^j = I$ if and only if $\lambda_\ell^j = 1$ for $1 \le \ell \le n$. Note that $\lambda_1, \dots, \lambda_n$ are the eigenvalues of A, because A is similar to D.

12. Show that $(xyx^{-1})^j = xy^jx^{-1}$ for all positive integers j. Then note that $xy^jx^{-1} = e$ implies (multiply on the left by x^{-1} and on the right by x) $y^j = x^{-1}ex = x^{-1}x = e$. Therefore $(xyx^{-1})^j = e$ if and only if $y^j = e$. Thus xyx^{-1} and y have the same order.

13. a) Check that $A^2 = -I$, $A^3 = -A$ and $A^4 = (-I)^2 = I$. Thus A has order 4. Next, note that $B^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ and $B^3 = I$. Thus B has order 3.

13. b) The subgroup $H = \langle\, A, B \,\rangle$ generated by A and B contains the product $AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Show that $(AB)^j = \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix} \ne I$. Therefore AB has infinite order and H contains the infinite cyclic group $\langle\, AB \,\rangle$ and therefore H is itself infinite.

13. c) Since A has order 4 and B has order 3, both A and B belong to the set H' of elements of G that have finite order. As shown in part b), the product AB has infinite order. Therefore H' is not a subgroup of G.

14. Let $A \in GL_n(\mathbb{F}_p)$. Following the hint, the number of choices for the first row of A is equal to the number of nonzero vectors in $\mathbb{F}_p^n$, and that is equal to $p^n - 1$. The second row of A can be any vector that does not belong to the span of the first row. The span of the first row contains p vectors. So there are $p^n - p$ choices for the second row. The span of the first and second rows contains p^2 vectors, so we have $p^n - p^2$ choices for the third row. Continuing, we see that there are a total of

$$(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}) = p^{n(n-1)/2}(p - 1)(p^2 - 1) \cdots (p^n - 1)$$

choices for A.

15. a) Let $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. and $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Then $\varphi(A) = I$, $\varphi(B) = I$ and $\varphi(AB) = -I \neq \varphi(A)\varphi(B)$. Thus φ is not a homomorphism when $n = 2$. If $n \geq 3$, let $A' \in G$ be the matrix with $A'_{jk} = A_{jk}$ for $1 \leq j,k \leq 2$, $A_{jk} = 0$ if $j \geq 3$ or $k \geq 3$ and $j \neq k$, and $A_{jj} = 1$ if $j \geq 3$. Define B' similarly. Then show that $\varphi(A'B') \neq \varphi(A')\varphi(B')$ to verify that φ is not a homomorphism for $n \geq 3$.

15. b) If $A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ and $B = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}$ belong to G, then (omitting details)

$$\varphi(AB) = (|a\,a'|, (d\,d')^4) = (|a||a'|, d^4(d')^4) = (|a|, d^4)(|a'|, (d')^4) = \varphi(A)\varphi(B),$$

so φ is a homomorphism. Note that the identity element e' of G' is $e' = (1,1)$. If $A \in G$, then $\varphi(A) = (1,1)$ if and only if $|a| = 1$ and $d^4 = 1$. That is, A belongs to the kernel of φ if and only if $|a| = 1$ and $d \in \{ i, -i, 1, -1 \}$ (and b is any complex number). Since every nonzero complex number is of the form d^4 for some d, and a real number is of the form $|a|$ for some nonzero complex number a if and only if it is positive, the image of φ is the set (c, z) where c is a positive real number and z is a nonzero complex number.

15. c) Let $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix}$. Then $\varphi(A)\varphi(B) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\varphi(AB) = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$. Therefore φ is not a homomorphism.

16. a) Check that $J((AB)^t)^{-1}J^{-1} = J((B^tA^t)^{-1}J^{-1} = J(A^t)^{-1}(B^t)^{-1}J^{-1} = J(A^t)^{-1}J^{-1}J(B^t)^{-1}J$ to see that φ is a homomorphism.

16. b) Note that $\varphi(I) = JIJ^{-1} = I$ tells us that H is nonempty. Suppose that A, $B \in H$. Then

$$\begin{aligned}\varphi(AB^{-1}) &= J((AB^{-1})^t)^{-1}J^{-1} = J\,(A^t)^{-1}B^tJ^{-1} = (J(A^t)^{-1}J^{-1}(J(B^t)^{-1}J^{-1})^{-1} \\ &= \varphi(A)\varphi(B)^{-1} = A \cdot B^{-1},\end{aligned}$$

so $AB^{-1} \in H$. Therefore H is a subgroup of G.

16. c) Let $A \in G$. Note that

$$\varphi_1(A) = BJB^t(A^t)^{-1}(BJB^t)^{-1} = BJB^t(A^t)^{-1}(B^t)^{-1}J^{-1}B^{-1} = B\varphi(B^{-1}AB)B^{-1}.$$

It follows that $A \in H_1$ if and only if $A = B\varphi(B^{-1}AB)B^{-1}$. Multiplying on the left by B^{-1} and on the right by B, we get $A \in H_1$ if and only if $B^{-1}AB = \varphi(B^{-1}AB)$. Thus $A \in H_1$ if and only if $B^{-1}AB \in H$. Define $\psi : H_1 \to H$ by $\psi(A) = B^{-1}AB$, $A \in H_1$. Then $\psi(A_1A_2) = B^{-1}(A_1A_2)B = B^{-1}A_1B\,B^{-1}A_2B = \psi(A_1)\psi(A_2)$. Therefore ψ is a group homomorphism. Define $\dot{\psi} : H \to H_1$ by $\dot{\psi}(A) = BAB^{-1}$, $A \in H$. Now check that $\dot{\psi} \circ \psi$ is the identity map on H_1 and $\psi \circ \dot{\psi}$ is the identity map on H. This shows that $\dot{\psi}$ is an inverse of ψ. Therefore ψ is an isomorphism.

17. The set $GL_1(\mathbb{Q})$ is countable (there exists a bijective map from $GL_1(\mathbb{Q})$ to the set $\mathbb{N}$ of positive integers). If $GL_1(\mathbb{Q})$ and $GL_1(\mathbb{R})$ were isomorphic, then there would exist a bijective group homomorphism from $GL_1(\mathbb{Q})$ to $GL_1(\mathbb{R})$. Composing this bijection with a bijective map between $\mathbb{N}$ and $GL_1(\mathbb{Q})$ with the homomorphism, we obtain a bijective map from $\mathbb{N}$ to $GL_1(\mathbb{R})$. However $GL_1(\mathbb{R})$ is uncountable, so there does not exist a bijective map from $\mathbb{N}$ to $GL_1(\mathbb{R})$.

18. a) If the image of φ is abelian, then $\varphi(r)\varphi(s) = \varphi(s)\varphi(r)$. Because φ is a homomorphism, $rs = sr^{-1}$ implies that $\varphi(r)\varphi(s) = \varphi(s)\varphi(r)^{-1}$. If the image of φ is abelian, this is the same as $\varphi(r)\varphi(s) = \varphi(r)^{-1}\varphi(s)$. Multiplying both sides by $\varphi(s)^{-1}\varphi(r)$, we see that $\varphi(r)^2 = e'$. Suppose that $1 \leq j \leq n-1$. Then $\varphi(r^j)^2 = \varphi(r)^{2j} = (e')^j = e'$. Since $s^2 = e$ and φ is a homomorphism, we have $\varphi(s)^2 = \varphi(e) = e'$. Finally $\varphi(r^j s)^2 = \varphi(r^j)^2 = \varphi(s)^2 = e' \cdot e' = e'$. This shows that if the image of φ is abelian, then $\varphi(x)^2 = e'$ for every $x \in D_n$.
For the other direction, suppose that $\varphi(x)^2 = e'$ for every $x \in D_n$. Then $\varphi(x)^{-1} = \varphi(x)$ for every $x \in D_n$. Let x, $y \in D_n$. Take $(\varphi(x)\varphi(y))^2 = \varphi(x)\varphi(y)\varphi(x)\varphi(y) = e'$ and multiply by $\varphi(y)\varphi(x)$ to get (details omitted) $\varphi(x)\varphi(y) = \varphi(y)\varphi(x)$.

18. b) Suppose that n is odd and $\varphi(r) \neq e'$. Because $e' = \varphi(e) = \varphi(r^n) = (\varphi(r))^n$, the order of $\varphi(r)$ must divide n (using the fact that if x is a group element such that $x^n = e$ for some positive integer n, then the order of x divides n). By part a), if the image of φ is abelian, then $\varphi(r)^2 = e'$. This implies that the order of $\varphi(r)$ is 1 or 2. Since we already know that $\varphi(r)$ cannot have order 2, since 2 does not divide n, we must have $\varphi(r) = e'$. This contradicts the assumption that $\varphi(r) \neq e'$. Hence the image of φ cannot be abelian.

18. c) As we saw in part b), $\varphi(r)$ has order dividing 9. That is, $\varphi(r)$ has order 1, 3 or 9. If $\varphi(r^3) = (\varphi(r))^3 \neq e'$, then $\varphi(r)$ has order 9. Suppose that $x = r^j$ belongs to the kernel of φ, and $0 \leq j \leq 8$. That is, suppose $\varphi(r^j) = \varphi(r)^j = e'$. This implies that the order of $\varphi(r)$ divides j. But the order of $\varphi(r)$ is 9. Then $\varphi(r)^j = e'$ and $j \leq 8$ imply that $j = 0$ (since $\varphi(r)$ has order 9). Therefore $r^j = e$. Now suppose that $\varphi(r^j s) = e'$. We know that $\varphi(s)^2 = \varphi(s^2) = \varphi(e) = e'$, so

$$\varphi(r^j) = \varphi(r^j)\varphi(s)\varphi(s) = \varphi(r^j s)\varphi(s) = e'\varphi(s) = \varphi(s).$$

If $\varphi(s) = e$, then $\varphi(r^j) = e'$, which implies that $j = 0$. But $rs = sr^{-1}$ implies that $\varphi(r)\varphi(s) = \varphi(s)\varphi(r)^{-1} = \varphi(s)\varphi(r)^8$ and $\varphi(s) = e$ imply that $\varphi(r) = \varphi(r)^8$. Mutliplying by $\varphi(r)^{-1}$, we get $\varphi(r)^7 = e'$, which is impossible. Therefore $\varphi(s) \neq e'$. We have shown that if $x \in D_9$ and $\varphi(x) = e'$, then $x = e$. That is, the kernel of φ is $\{e\}$. Now apply the result that tells us that the kernel of φ is $\{e\}$ if and only if φ is one to one.

19. a) Note that $\varphi(r^j) = \varphi(r)^j = (r^{-1})^j = r^{-j}$, $\varphi(s)^2 = s^2 = e$, $\varphi(rs) = r^{-1}s = \varphi(r)\varphi(s)$, and $\varphi(s)\varphi(r)^{-1} = sr = r^{-1}s$. Thus φ is a homomorphism. Since the image of φ is all of D_n (we can write each element of D_n in the form $\varphi(x)$ for some $x \in D_n$ - check this for yourself), we see that φ is onto. It follows that φ is bijective. Hence φ is an isomorphism. In particular, the kernel of φ is $\{e\}$. (*Alternate answer*: Check that $\varphi(x) = sxs^{-1}$ for each $x \in D_n$ and use the fact that if $y \in G$, then the map $\varphi(x) = yxy^{-1}$ from G to G is a group isomorphism.)

19. b) Similar to part a). First, show that φ is a homomorphism: check that $\varphi(r^j) = \varphi(r^j)$, $0 \leq j \leq n-1$, $\varphi(s)^2 = e$, and $\varphi(s)\varphi(r)^{-1} = \varphi(r)\varphi(s)$... Next, verify that the image of φ is all of D_n, which implies that φ is bijective, and the kernel of φ is $\{e\}$. (Or show that $\varphi(x) = rxr^{-1}$ for all $x \in D_n$...)

19. c) Note that $rs = \varphi(rs)$ and $r^{-1}s = \varphi(r)\varphi(s)$. If φ was a homomorphism, this would imply that $rs = r^{-1}s$. Multiplying both sides by s we get $r = r^{-1}$, which is false. Therefore φ is not a homomorphism.

19. d) Note that $\varphi(r^j) = r^{2j} = (r^2)^j = \varphi(r)^j$ and $\varphi(r^j s) = r^{2j}s = \varphi(r)^j\varphi(s)$, for $0 \leq j \leq n-1$, and also $\varphi(r)\varphi(s) = r^2 s = sr^{-2} = \varphi(s)\varphi(r)^{-1}$. Thus φ is a homomorphism. Suppose that $\varphi(r^j) = e$. Then $r^{2j} = e$ implies that n divides $2j$, since r has order n. If n is odd, then this forces n to divide j, which in turn forces $j = 0$. If n is even, will have $j = 0$ or $j = n/2$.

Omitting a few details (i.e. checking that $r^j s$ is not in the kernel of φ), we then see that the kernel of φ is $\{ e \}$ when n is odd and it is $\{ e, r^{n/2} \}$ when n is even.

20. Let $x \in G$. Then x cannot have infinite order, because if it did, then the subgroup $\langle x \rangle$ of G generated by x would be an infinite subgroup of the finite group G. Thus x has finite order. Let m be the order of x. Let $A = \varphi(x)$. Because φ is a homomorphism, we have $I = \varphi(e) = \varphi(x^m) = \varphi(x)^m = A^m$ where I is the $n \times n$ identity matrix. This is the same as $A^m - I = 0$. Therefore, setting $g(t) = t^m - 1$, we see that $g(A) = 0$. Let $p(t)$ be the minimal polynomial of the matrix A. Then $g(A) = 0$ implies that $p(t)$ divides $g(t)$. Let $\zeta = e^{2\pi i/m}$. The zeros of $g(t) = t^m - 1$ are the numbers ζ^j, $0 \le j \le m - 1$ and

$$g(t) = (t - \zeta)(t - \zeta^2) \cdots (t - \zeta^{m-1})(t - 1).$$

Since $g(t)$ has m distinct zeros and $p(t)$ divides $g(t)$, the polynomial $p(t)$ has distinct zeros. According to a theorem, from class, the fact that $p(t)$ has distinct zeros implies that the matrix A is diagonalizable.

21. a) Let j be chosen so that $r^j s \in H$. Because $r^j s \in H$ and H is a normal subgroup, we must have $x(r^j s)x^{-1} \in H$ for all $x \in D_n$. Take $x = r$ to get

$$r(r^j s)r^{-1} = r^{j+1} s r^{-1} = r^{j+1} r s = r^{j+2} s \in H.$$

Next, since $r^{j+2}s$ and $r^j s$ belong to H and H is a subgroup of G imply that $r^{j+1}s \cdot r^j s \in H$. That is, $r^{j+2} s r^j s = r^{j+2} r^{-j} s^2 = r^2 s^2 = r^2 e = r^2 \in H$.

22. b) Suppose that n is odd. Note that $(r^2)^{(n+1)/2} = r^n r = er = r$ implies that r belongs to the cyclic subgroup generated by r^2. But, since $r^2 \in H$ (see part b)), this implies $r \in H$. Now we have $r \in H$ and $r^j s \in H$ (for some j). This implies that $s = (r^j) r^j s \in H$. We have shown that if n is odd, then r, $s \in H$. Because H is a subgroup of D_n and $D_n = \langle r, s \rangle$, it follows that $D_n \subset H \subset D_n$. Thus $H = D_n$ when n is odd.

23. a) Suppose that n is even. Let $H = \langle r^2, s \rangle$. We must show that if $x \in D_n$ and $y \in H$, then $xyx^{-1} \in H$. To do that, is enough to show that xr^2x^{-1} and xsx^{-1} belong to H for all $x \in D_n$. Note that $r\, r^2 r^{-j} = r^2$ and $(r^j s) r^2 (r^j s)^{-1} = (r^2)^{-1} \in H$. Also, $r^j s r^j = s \in H$, $(r^j s) s (r^j s)^{-1} = r^{2j} s \in H$.

23. b) Suppose that n is even and $n \ge 6$. Let $H = \langle r^2, s \rangle$. Rough idea: Let r_1 be a rotation in $D_{n/2}$ and let s_1 be a reflection in $D_{n/2}$. Define $\varphi : H \to D_{n/2}$ by $\varphi(r^{2j}) = r_1^j$, $\varphi(r^{2j}s) = r_1^j s_1$, $0 \le j \le n/2$. Verify that φ is an isomorphism.

23. c) Let $H = \langle rs, r^2 s \rangle$. To show that $H = D_n$, it's enough to show that r, $s \in H$ and then use the fact that r and s generate D_n. Note that $r = (r^2 s)(rs) \in H$, because H is subgroup and $r^2 s$, $rs \in H$. Now H is a subgroup, so $r \in H$ implies that $r^{-1} \in H$. Finally, note that $r^{-1}(rs) = s$ belongs to H because r^{-1} and rs belong to H.

24. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an element of U_2. The rows of A must form an orthonormal basis for $\mathbb{C}^2$ relative to the standard inner product. Therefore

$$a\bar{a} + b\bar{b} = c\bar{c} + d\bar{d} = 1, \quad a\bar{c} + b\bar{d} = 0.$$

We also know that $\det A \cdot \overline{\det A} = 1$. Now do some algebra to show that if we set $z = a$ and $w = b$ and choose θ so that $\det A = e^{i\theta}$, then $c = -e^{i\theta}\bar{w}$ and $d = e^{i\theta}\bar{z}$.

25. Suppose that $\varphi : D_8 \to GL_2(\mathbb{C})$ be a homomorphism having the property that $\varphi(r) = A = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$.

a) Let $B = \varphi(s)$. Because φ is a homomorphism, we must have $\varphi(rs) = AB = \varphi(s)\varphi(r)^{-1} = BA^{-1}$. If $AB = BA$, then this would imply $A = A^{-1}$. But $A^{-1} = -A$. So $AB \neq BA$. This is the same as $\varphi(r)\varphi(s) \neq \varphi(s)\varphi(r)$. Thus the image of φ is nonabelian.

b) Use the relations $B^2 = I$ (follows from $s^2 = e$ and φ is a homomorphism) and $AB = BA^{-1}$ (from part a)) and do some algebra to show B has the form indicated in the question.

c) Check that $A = \varphi(r)$ has order 4. Use this to prove that r^j belongs to kernel of φ if and only if $j = 0$ or $j = 4$. If $\varphi(r^j s) = I$, then $A^j B = I$ implies $B = (A^j)^{-1}$- using the form of A and B, show that this can't happen. So the kernel of φ is $\{ e, r^4 \}$.

d) Let H be the image of φ. Then

$$H = \langle A, B \rangle = \{ I, A, A^2, A^3, B, AB, A^2B, A^3B \}.$$

Let r_1 be a rotation of order 4 in D_4, and let s_1 be a reflection in D_4. Define $\psi : H \to D_4$ by $\psi(A^j) = r_1^j$ and $\psi(A^j B) = r_1^j s_1$, $0 \leq j \leq 4$. Then show that ψ is a homomorphism and ψ is one to one (details omitted). Because both H and D_4 have order 8, it follows that ψ is an isomorphism.

25. Let $\varphi : D_8 \to GL_2(\mathbb{C})$ be a map such that $\varphi(r) = A = \begin{pmatrix} 0 & 1 \\ i & 0 \end{pmatrix}$. If φ was a homomorphism, then, letting $B = \varphi(s)$, we would have $B^2 = I$ (so $B = B^{-1}$) and $\varphi(rs) = AB = BA^{-1} = \varphi(sr^{-1})$. This implies that $A = BA^{-1}B^{-1}$. In particular A is similar to A^{-1}. Taking determinants we get $\det A = \det(A^{-1})$. That is, $(\det A)^2 = 1$. Calculating, we see that $(\det A)^2 = (-i)^2 = -1 \neq 1$. Therefore A is not similar to A^{-1}, and φ cannot be a homomorphism.

26. Suppose that $m \geq 3$. Suppose that D_m is isomorphic to a subgroup of D_n. Since isomorphisms preserve orders of elements and D_m contains at least one element of order m, there must be an element of D_n that has order m. Now all elements in D_n of the form $r^j s$ have order 2. So an element of D_m of order m would map to an element of D_n of the form r^j, $1 \leq j \leq n$, where r^j would have order m. Note that each element r^j has order dividing n, because $(r^j)^n = (r^n)^j = e^j = e$. Therefore m must divide n.
For the other direction, suppose that $m \geq 3$ and m divides n. Let r_1 be a rotation of order m in D_m and let s_1 be a reflection in D_m. Let $H = \langle r^{n/m}, s \rangle$ be the subgroup of D_n generated by $r^{n/m}$ and s. Define $\varphi : D_m \to H$ by $\varphi(r_1^j) = (r^{n/m})^j$ and $\varphi(r_1^j s_1) = (r^{n/m})^j s$, $0 \leq j \leq m-1$. Show that φ is an isomorphism (details omitted).

27. a) (Details omitted.) Check that H is closed under multiplication. Applying Question 10a), we see that H is a subgroup of D_6. Because $s(rs)s = r^{-1}s \cdot e = r^5 s \notin H$ and $rs \in H$, we see that H is not normal in D_6.

27. b) (Details omitted.) Check that rs and s belong to H and $(rs)s = r$ does not belong to H. Therefore H is not a subgroup of D_6.

27. c) Suppose that $r^j s \in H$. Since H is normal in D_n, we must have $r(r^j s)r^{-1} = r^{1+j+1}s = r^{j+2}s \in H$. Because H is a subgroup, the product $(r^{j+2}s)(r^j s)$ belongs to H. That is, $r^{j+2}r^{-j}s \cdot s = r^2 \cdot e = r^2 \in H$.

27. d) According to part c), if H is a normal subgroup of D_6 and $rs \in H$, then $r^2 \in H$. So $\langle rs, r^2 \rangle \subset H$. Check that $\langle rs, r^2 \rangle = \{ e, rs, r^3 s, r^5 s, r^2, r^4 \}$ and is normal in D_6. Note that the order of $\langle rs, r^2 \rangle$ is 6 and the order of D_6 is twelve. This implies, by Lagrange's Theorem, that

6 divides the order of H and the order of H divides 12. Therefore the order of H is 6 or 12. Either $H = \langle rs, r^2 \rangle$ or $H = D_6$.

28. a) Assume that φ is a homomorphism. Then $\varphi(s)\varphi(r)\varphi(s)^{-1} = \varphi(r)$ because $GL_1(\mathbb{C})$ is abelian and $\varphi(s)\varphi(r)\varphi(s)^{-1} = \varphi(r)^{-1}$ because φ is a homomorphism. Therefore $i^{-1} = i$. This is false (actually $i^{-1} = -i \neq i$). Contradiction.

28. b), c) These parts were discussed in class.

29. Note that e has order 1, so $e \in H$, That is, H is nonempty. We may apply the subgroup test. Let x, $y \in H$. Let m be the order of x and let n be the order of y. Since $(y^{-1})^\ell = (y^\ell)^{-1}$ for all positive integers ℓ, we see that $(y^{-1})^\ell = e$ if and only if $y^\ell = e$. It follows that n is the order of y^{-1}. Because G is abelian, we know that $xy^{-1} = y^{-1}x$. This implies that

$$(xy^{-1})^\ell = (xy^{-1})(xy^{-1}) \cdots (xy^{-1}) = x^\ell (y^{-1})^\ell$$

for any positive integer ℓ. From this we see that

$$(xy^{-1})^{mn} = (x^m)^n ((y^{-1})^n)^m = e^n \cdot e^m = e \cdot e = e.$$

Therefore xy^{-1} has finite order for all x, $y \in H$. According to the subgroup test, H is a subgroup of G.