Math 301 **Sketch of Solutions for Midterm 1** **03/29/04**

Part A.

Indicate whether each of the following statements is true or false. No work is required in this problem.

1. Since each permutation has an inverse, the product of all permutations in S_n is the identity permutation.

   FALSE; even S_2 disproves this: $\varepsilon(12) = (12) \neq \varepsilon$. Note that involutions (i.e. permutations that are their own inverses, i.e. are of order 2) appear only once, not twice, in such a product. Note also that S_n is nonabelian for $n \geq 3$ and inverses are not required to be consecutive factors in such a product.

2. Upper-triangular matrices with all 1's on the diagonal form a subgroup of $SL(n, \mathbb{R})$.

   TRUE; a product of upper-triangular matrices is upper triangular, and the diagonal entries of the product are products of their diagonal entries in the same positions, hence also all 1's.

3. $(\mathbb{Z}, *)$, where $a * b = ab + a + b$, is a group.

   FALSE; if true, then $0 * a = a * 0 = a$, so 0 is the identity element, but $(-1) * a = a * (-1) = -1 \neq 0$ for any integer a, so -1 does not have an inverse under $*$.

4. Let G be a group and H a subgroup of G. Define the normalizer $N(H)$ of H by $N(H) = \{g \in G \mid g^{-1}Hg = H\}$. Then $N(H) = \bigcap_{h \in H} C(h)$, where $C(h)$ is the centralizer of the element h.

   FALSE; $\bigcap_{h \in H} C(h)$ consists of elements $g \in G$ which fix each element of H (i.e. $g^{-1}hg = h$ for any $h \in H$). On the other hand, for g to be an element of $N(H)$, we only need to know that, given any $h \in H$, we have $g^{-1}hg = h'$ for some $h' \in H$, not necessarily $g^{-1}hg = h$.

5. Not all groups of order 4 are cyclic.

   TRUE; e.g. the group of symmetries of a rectangle $V = \{e, x, y, z \mid x^2 = y^2 = z^2 = e,\ xy = yx = z,\ xz = zx = y,\ yz = zy = x\}$ is not cyclic, since every nonidentity element of V is of order 2 (see Problem B2 below). V is called the *Klein's 4-group* (the notation V comes from German *vier* meaning "four").

Part B.

1. Here are some entries of a Cayley table for a group G of order 6.

	u	v	w	x	y	z
u						z
v		w			x	
w			v			
x		y		u		
y						
z						

   Determine the rest of the entries of the above Cayley table. What known groups are isomorphic to G?

   We have $uz = z$, so $u = e$. Now $w = v^2$ and $v = w^2$, so $v = (v^2)^2 = v^4$, and hence $v^3 = e$, so $vw = wv = e$, i.e. $w = v^{-1}$. We also have $x^2 = u = e$, and $xv = y$, $vy = x$, so $vxv = x$, i.e. $vx = xv^{-1} = xw$. Now what is xw? We have $xw \neq x = xe$ since $x \neq e$; $xw \neq w = ew$ since $w \neq e$; $xw \neq e = xx$ since $w \neq x$; $xw = vx \neq v = ve$ since $x \neq e$; and $xw \neq y = xv$ since $w \neq v$. Therefore, $xw = z$. Thus, we have $G = \{e, v, v^2, x, xv, xv^2 \mid v^3 = e,\ x^2 = e,\ vx = xv^{-1}\}$, so $G \cong S_3$. The rest of the table can be filled out just as for S_3 (or D_3).

	u	v	w	x	y	z
u	u	v	w	x	y	z
v	v	w	u	z	x	y
w	w	u	v	y	z	x
x	x	y	z	u	v	w
y	y	z	x	w	u	v
z	z	x	y	v	w	u

2. Let V be a group of symmetries of a rectangle. Prove that V is a subgroup of D_4. What are the elements of V? What is the order of V? Write the Cayley table for V. What is the order of each element of V? Is V abelian? Is V cyclic?

   A square is a type of rectangle, so all symmetries of a rectangle are also symmetries of the square. Therefore, V is a subset of D_4. But V is also a group, so V is a subgroup of D_4. The symmetries in V are the identity, the two reflections along the vertical and horizontal axes of symmetry and the rotation by 180°. If we write $D_4 = \{e, \rho, \rho^2, \rho^3, \phi, \phi\rho, \phi\rho^2, \phi\rho^3 \mid \phi^2 = \rho^4 = e,\ \rho\phi = \phi\rho^{-1}\}$, then $V = \{e, \rho^2, \phi, \phi\rho^2\}$. An equivalent description of V is given in Problem A5. Since $\phi\rho^2 = \rho^2\phi$, it is easy to check that V is abelian. Similarly, it is easy to check that every element except e has order 2, so V cannot be cyclic since it does not contain an element of order $4 = |V|$. The Cayley table for V is given below.

	e	ρ^2	ϕ	$\phi\rho^2$
e	e	ρ^2	ϕ	$\phi\rho^2$
ρ^2	ρ^2	e	$\phi\rho^2$	ϕ
ϕ	ϕ	$\phi\rho^2$	e	ρ^2
$\phi\rho^2$	$\phi\rho^2$	ϕ	ρ^2	e

3. (a) Let G be a group and let $\rho, \phi \in G$. Prove by induction that $\rho\phi = \phi\rho^{-1}$ implies $\rho^n\phi = \phi\rho^{-n}$ for any integer n. *Hint:* Use induction on n.

   The results is obviously true for $n = 0, 1$. Suppose it is true for some n, i.e. $\rho^n\phi = \phi\rho^{-n}$. Then $\rho^{n+1}\phi = \rho\rho^n\phi = \rho\phi\rho^{-n} = \phi\rho^{-1}\rho^{-n} = \phi\rho^{-(n+1)}$, so the result is also true for $n+1$. Thus, by induction on n, $\rho^n\phi = \phi\rho^{-n}$ for any integer $n \geq 0$.

   Now let $n < 0$, then $-n > 0$, so $\rho^{-n}\phi = \phi\rho^{-(-n)} = \phi\rho^n$. Now, multiplying both sides by ρ^n on the left and by ρ^{-n} on the right, we get $\phi\rho^{-n} = \rho^n\phi$ as desired.

   (b) Determine $C(\phi)$ in $D_4 = \{e, \rho, \rho^2, \rho^3, \phi, \phi\rho, \phi\rho^2, \phi\rho^3 \mid \phi^2 = \rho^4 = e,\ \rho\phi = \phi\rho^{-1}\}$.

   Since D_4 has only 8 elements, one can simply check which ones commute with ϕ. Those turn out to be $e, \phi, \rho^2, \phi\rho^2$. Thus, $C(\phi) = \{e, \phi, \rho^2, \phi\rho^2\}$.

   (c) Determine $C(\phi)$ in $D_5 = \{e, \rho, \rho^2, \rho^3, \rho^4, \phi, \phi\rho, \phi\rho^2, \phi\rho^3, \phi\rho^4 \mid \phi^2 = \rho^5 = e,\ \rho\phi = \phi\rho^{-1}\}$.

   Similarly, we can check that only e and ϕ commute with ϕ. Thus, $C(\phi) = \{e, \phi\}$.

   (d) (extra) Determine $C(\phi)$ in $D_n = \{\phi^i\rho^j \mid i = 0, 1,\ j = 0, 1, \ldots, n-1,\ \phi^2 = \rho^n = e,\ \rho\phi = \phi\rho^{-1}\}$. *Hint:* The answer depends on whether n is even or odd.

   Of course, checking each integer n is not very efficient, so we need another solution. Obviously, any power of ϕ commutes with ϕ, hence $e, \phi \in C(\phi)$.

   Does any power ρ^k $(0 \leq k \leq n-1)$ of ρ other than e commute with ϕ? If it does, then $\phi\rho^k = \rho^k\phi$. But $\rho\phi = \phi\rho^{-1}$, so by part (a), $\rho^k\phi = \phi\rho^{-k}$.

   Hence, $\phi\rho^k = \rho^k\phi = \phi\rho^{-k}$, so $\rho^k = \rho^{-k}$, i.e. $\rho^{2k} = e$, so $2k$ is divisible by $n = |\rho|$. Since $0 \leq 2k \leq 2n-2$, we have $2k = 0$ (i.e. $k = 0$) or $2k = n$. The solution $k = 0$ yields $\rho^0 = e$, so we need $k = n/2$, which is an integer if and only if n is even. Thus, if n is odd, only e and ϕ commute with ϕ, so $C(\phi) = \{e, \phi\}$ for odd n. If n is even, then $e, \phi, \rho^{n/2} \in C(\phi)$, so $\phi\rho^{n/2} \in C(\phi)$ as well since $C(\phi)$ is a group. Solving $\phi(\phi\rho^l) = (\phi\rho^l)\phi$, we similarly get $l = n/2$, so we found all the elements which commute with ϕ. Thus, $C(\phi) = \{e, \phi, \rho^{n/2}, \phi\rho^{n/2}\}$ for even n.

4. Let G be a group generated by two elements σ and τ. (In other words, G is the group that consists of all possible products of any number of factors each of which is one of σ, τ, σ^{-1}, τ^{-1}. Alternatively, G is the smallest group that contains σ and τ.)

(a) If α is an element of G, explain carefully how you can conclude that α lies in the center $Z(G)$ of G provided you know that $\alpha\sigma = \sigma\alpha$ and $\alpha\tau = \tau\alpha$. (*Hint:* Use induction.)

We need to prove that, for any $g \in G$, if $\alpha\sigma = \sigma\alpha$ and $\alpha\tau = \tau\alpha$, then $\alpha g = g\alpha$. Each element $g \in G$ is a product of a string of $n \geq 0$ factors each of which is σ, τ, σ^{-1} or τ^{-1}. Our proof will be by induction on n.

Induction Base. The implication is clearly true for $g = e$, $g = \sigma$ and $g = \tau$. Also, $\alpha\sigma = \sigma\alpha$ implies $\sigma^{-1}\alpha\sigma\sigma^{-1} = \sigma^{-1}\sigma\alpha\sigma^{-1}$, i.e. $\sigma^{-1}\alpha = \alpha\sigma^{-1}$ Similarly, $\alpha\tau = \tau\alpha$ implies $\tau^{-1}\alpha\tau\tau^{-1} = \tau^{-1}\tau\alpha\tau^{-1}$, i.e. $\tau^{-1}\alpha = \alpha\tau^{-1}$. Thus, our statement is true for $g = \sigma^{-1}$ and $g = \tau^{-1}$ as well, in other words, for $n = 0, 1$.

Induction Step. Suppose now that our statement is true for all products g' of at most $n-1$ factors from $\{\sigma, \tau, \sigma^{-1}, \tau^{-1}\}$. Let g be a product of n factors from $\{\sigma, \tau, \sigma^{-1}, \tau^{-1}\}$. Then $g = g'x$, where g' is as above and $x \in \{\sigma, \tau, \sigma^{-1}, \tau^{-1}\}$, so we have $g'\alpha = \alpha g'$ by induction hypothesis, and hence, $g\alpha = g'x\alpha = g'\alpha x = \alpha g'x = \alpha g$. Therefore, our statement is true for for all products g of n factors from $\{\sigma, \tau, \sigma^{-1}, \tau^{-1}\}$.

Thus, by induction on n, our statement is true for any n, i.e. for any element $g \in G$.

(b) Now suppose that G is generated by σ and τ, and that $\sigma^5 = e$, $\tau^3 = e$, and $\sigma^{-1}\tau = \tau\sigma$. Show that τ^2 lies in the center of G. (*Hint:* Use part (a).)

By part (a), we only need to show that τ^2 commutes with the generators σ and τ. Obviously, $\tau^2\tau = \tau^3 = \tau\tau^2$, so τ^2 commutes with τ. Also, $\tau\sigma = \sigma^{-1}\tau$, so $\sigma\tau\sigma = \tau$, and hence $\sigma\tau = \tau\sigma^{-1}$. Therefore, $\tau^2\sigma = \tau\tau\sigma = \tau\sigma^{-1}\tau = \sigma\tau\tau = \sigma\tau^2$, so τ^2 commutes with σ as well. Thus, by part (a) $\tau^2 \in Z(G)$.

(c) Now show that τ itself lies in the center of G.

Recall that the center $Z(G)$ of G is a subgroup of G. From part (b), $\tau^2 \in Z(G)$, so $\tau = e\tau = \tau^3\tau = \tau^4 = \tau^2\tau^2 \in Z(G)$.

(d) From your results above and $\sigma^4\tau = \tau\sigma$, conclude that $\sigma^3 = e$.

From part (c), $\tau \in Z(G)$, so τ commutes with any element of G, in particular, $\tau\sigma = \sigma\tau$. Thus, $\sigma^{-1}\tau = \tau\sigma = \sigma\tau$, so $\sigma^{-1} = \sigma$, i.e. $\sigma^2 = e$.

(e) Finally, show that G is actually generated by τ alone, and G is in fact cyclic of order 3.

From part (d), $\sigma^2 = e$, so $e = e^3(\sigma^2)^3 = \sigma^6 = \sigma^5\sigma = e\sigma = \sigma$. Thus, $\sigma = e$. Since $\sigma = e$, and any $g \in G$ is a product of some string of σ, τ, σ^{-1} and τ^{-1}, we get that each $g \in G$ is a product of a string of τ's, i.e. G is generated by τ alone, i.e. $G = (\tau)$ and hence G is cyclic. But $\tau^3 = 1$, so the distinct elements of G are $1, \tau, \tau^2$. Hence G is cyclic of order 3.