Foundations of Algebra — Name (please print) ______________________

Exam II, June 28, 2004

Clearly justify each step in your answers.

I. (10) Assume that e is an identity element for an operation $*$ on a set S. If $a, b \in S$ and $a * b = e$, then a is said to be a *left inverse* of b and b is said to be a *right inverse* of a. Prove that if $*$ is associative, b is a left inverse of a, and c is a right inverse of a, then $b = c$.

Solution. We have

$$\begin{aligned} b * a &= e && \text{because } b \text{ is a left inverse of } a \\ (b * a) * c &= e * c = c && \text{because } e \text{ is the identity} \\ b * (a * c) &= c && \text{because } * \text{ is associative} \\ b * e &= c && \text{because } c \text{ is a right inverse of } a \\ b &= c && \text{because } e \text{ is the identity} \end{aligned}$$

II. (5) Verify that the set $\{3m : m \in \mathbb{Z}\}$ is a group under addition. Identify clearly the properties of $\mathbb{Z}$ that you are using.

Solution.

Nonempty. $3 = 3 \cdot 1$ so the set is nonempty.

Closed under addition: Let $3m_1, 3m_2$ where $m_1, m_2 \in \mathbb{Z}$ be any two elements in $\{3m : m \in \mathbb{Z}\}$. Then $3m_1 + 3m_2 = 3(m_1 + m_2) \in \{3m : m \in \mathbb{Z}\}$, so it is closed under addition.

Associativity. Addition is associative in this set because $\{3m : m \in \mathbb{Z}\} \subseteq \mathbb{Z}$ and addition is associative in $\mathbb{Z}$.

Identity. $0 = 3 \cdot 0 \in \{3m : m \in \mathbb{Z}\}$. Now, since we have $0 + k = k + 0 = k$ for all $k \in \mathbb{Z}$, it follows that 0 is the identity in $\{3m : m \in \mathbb{Z}\}$ as well.

Inverse. For $3m$, $m \in \mathbb{Z}$ we have $-3m = 3(-m)$, where $-m \in \mathbb{Z}$ as well and $3m + 3(-m) = 3(-m) + 3m = 0$, so $3(-m)$ is the inverse of $3m$.

Therefore, $\{3m : m \in \mathbb{Z}\}$ is a group under addition.

III. (10) Let $G = \{x, y, z, w\}$ with operation $*$ be a group whose identity is x. Complete the following Cayley tables for G in such a way that in both cases $*$ is commutative, that is G is an abelian group.

a) (5)

$*$	x	y	z	w
x	x	y	z	w
y	y	x	**w**	**z**
z	z	**w**	x	**y**
w	w	**z**	**y**	x

b) (5)

$*$	x	y	z	w
x	x	y	z	w
y	y	**z**	**w**	x
z	z	**w**	x	**y**
w	w	x	**y**	**z**

IV. (10) Write each of the following as a single cycle or a product of disjoint cycles (each part is worth 5 points):

a) $(1\quad 2\quad 3)^{-1}(2\quad 3)(1\quad 2\quad 3) = (1\quad 3\quad 2)(2\quad 3)(1\quad 2\quad 3) = (1\quad 2)$
Since $(1\quad 2\quad 3)^{-1} = (1\quad 3\quad 2)$
Or, using the *two-row form* representation of cycles:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{-1} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

b) $(2\quad 4\quad 5)(1\quad 3\quad 5\quad 4)(1\quad 2\quad 5) = (1\quad 4)(2\quad 5\quad 3)$
Or, using the *two-row form* representation of cycles:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix}$$

V. (10) Let $S = \{1, 2, 3, 4\}$ and $G = S_4$. Let T be a subset of S and write G_T for the subgroup of G consisting of the permutations $\alpha \in G$ such that $\alpha(t) = t$ for each $t \in T$. Find G_T for the following choices of T.

a) (5) $T = \{1, 4\}$
$G_T = \{(1), (2\quad 3)\}$

b) (5) $T = \{2, 3, 4\}$
$G_T = \{(1)\}$

VI. Verify that the set $\{\alpha_{1,b} : b \in \mathbb{R}\}$ is a subgroup (for the operation of composition of mappings) of the group
(5) $\{\alpha_{a,b} : a, b \in \mathbb{R}\ a \neq 0\}$, where the mapping $\alpha_{a,b} : \mathbb{R} \to \mathbb{R}$ is defined for $x \in \mathbb{R}$ by $\alpha_{a,b}(x) = ax + b$.

Solution.

Nonempty. Since $\alpha_{1,0}$, given by $\alpha_{1,0}(x) = x$ for $x \in \mathbb{R}$ is in the set, it is nonempty.

Closed under composition. For $x \in \mathbb{R}$ we have $\alpha_{1,b} \circ \alpha_{1,c}(x) = \alpha_{1,b}(x+c) = x+c+b$, so $\alpha_{1,b} \circ \alpha_{1,c} = \alpha_{1,b+c}$. Thus, $\{\alpha_{1,b} : b \in \mathbb{R}\}$ is closed under composition.

Inverse. If $\alpha_{1,b} \in \{\alpha_{1,b} : b \in \mathbb{R}\}$ then $\alpha_{1,-b} \in \{\alpha_{1,b} : b \in \mathbb{R}\}$ as well since $b \in \mathbb{R}$ implies $-b \in \mathbb{R}$. We have, for each $x \in \mathbb{R}$, $\alpha_{1,b} \circ \alpha_{1,-b}(x) = \alpha_{1,b}(x - b) = x + b - b = x = \alpha_{1,-b} \circ \alpha_{1,b}(x)$. Thus $\alpha_{1,-b}$ is the inverse of $\alpha_{1,b}$.