MAT 312/AMS 351: Applied Algebra
Solutions to Midterm II (70pts)

Problem 1 (10pts)

Answer Only: *circle* **T** *for TRUE and* **F** *for FALSE.*

(a) *The set $\mathbb{Z}^+$ of positive integers is a group under addition $+$.* **T** (**F**)
$1 \in \mathbb{Z}^+$ has no inverse with respect to $+$.

(b) *The set $4\mathbb{Z}$ of multiples of 4 is a group under addition $+$.* (**T**) **F**
$(4\mathbb{Z}, +)$ is closed under the associative $+$, contains the identity for $+$ (i.e. 0), and is closed under inverses for $+$ (i.e. negatives).

(c) *The set $\mathbb{Q}-\{0\}$ of nonzero rational numbers is a group under multiplication $*$.* (**T**) **F**
$(\mathbb{Q}-\{0\}, *)$ is closed under the associative $*$, contains the identity for $*$ (i.e. 1), and is closed under inverses for $*$ (i.e. reciprocals).

(d) *The set of $n \times n$ invertible matrices is a group under component addition $+$.* **T** (**F**)
This set is not closed under $+$: if M is invertible, then so is $-M$, but $M+(-M)$ is the zero matrix and thus is not invertible.

(e) *The set of $n \times n$ matrices is a group under matrix multiplication.* **T** (**F**)
The zero $n \times n$ matrix has no multiplicative inverse.

(f) *The groups $(\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +)$ and $(\mathbb{Z}_4, +)$ are isomorphic.* **T** (**F**)
$(\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +)$ contains no element of order 4, while $(\mathbb{Z}_4, +)$ does.

(g) *Every group of order 5 is abelian.* (**T**) **F**
Since 7 is prime, every group of order 5 is isomorphic to $(C_5, \cdot)$.

(h) *Every group of order 6 is abelian.* **T** (**F**)
The symmetric group S_3 is not abelian.

(i) *Every group of order 7 contains an element of order 7.* (**T**) **F**
Since 7 is prime, every group of order 7 is isomorphic to $(C_7, \cdot)$.

(j) *If a, b are elements of a group G, then $(ab)^{-1} = a^{-1}b^{-1}$.* **T** (**F**)
$(ab)^{-1} = b^{-1}a^{-1}$

Grading: X wrong answers; each correct answer 1pt

Problem 2 (4+4+4pts)

Answer Only: *only the answers appearing in the boxes provided below will be evaluated.*

Let $\pi, \sigma \in S_5$ *be the permutations*

$$\pi = (123)(45) \qquad \text{and} \qquad \sigma = (12)(345)\,.$$

(a) *Determine the permutations* $\pi\sigma$ *and* $\sigma\pi$ *in the two-row notation.*

$$\pi\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} \qquad \sigma\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 3 & 5 \end{pmatrix}$$

Grading: X wrong answers; each correct answer 2pts; if swapped, 2pts in total

(b) *Decompose* $\pi\sigma$ *and* $\sigma\pi$ *as products of disjoint cycles.*

$\pi\sigma =$ (135) $\qquad$ $\sigma\pi =$ (243)

Grading: X wrong answers; each correct answer 2pts; no penalty if based on answers in (a)

(c) *Determine the orders and signs of the permutations* $\pi, \sigma, \pi\sigma, \sigma\pi$.

	π	σ	$\pi\sigma$	$\sigma\pi$
order	6	6	3	3
sign	-	-	+	+

Grading: X wrong answers; each correct *column* 1pt

Problem 3 (2+3+5pts)

Let $(G,*)$ be a group with identity element e.

(a) *Let $a\in G$. Define what the order $\mathfrak{o}(a)$ of a in G means.*

$\mathfrak{o}(a)$ is the smallest $k\in\mathbb{Z}^+$ such that $a^k=e$; if such k does not exist, $\mathfrak{o}(a)\equiv\infty$.

Grading: 1pt for each part.

(b) *Let $a\in G$. Show that $\mathfrak{o}(a^{-1})=\mathfrak{o}(a)$.*

Since $(a^{-1})^{\mathfrak{o}(a)}=(a^{\mathfrak{o}(a)})^{-1}=e^{-1}=e$, $\mathfrak{o}(a^{-1})|\mathfrak{o}(a)$. Since $(a^{-1})^{-1}=a$, we also have $\mathfrak{o}(a)|\mathfrak{o}(a^{-1})$. Thus, $\mathfrak{o}(a^{-1})=\mathfrak{o}(a)$.

Grading: 1pt for each step.

(c) *Let $a\in G$, $i\in\mathbb{Z}^+$, and $d=\gcd(i,\mathfrak{o}(a))$. Show that $\mathfrak{o}(a^i)=\mathfrak{o}(a)/d$. Hint:* $\gcd(\mathfrak{o}(a)/d, i/d)=1$.

Since $d|i$ and $(a^i)^{\mathfrak{o}(a)/d}=(a^{\mathfrak{o}(a)})^{i/d}=e^{i/d}=e$, $\mathfrak{o}(a^i)|(\mathfrak{o}(a)/d)$. Since

$$a^{i\mathfrak{o}(a^i)}=(a^i)^{\mathfrak{o}(a^i)}=e,$$

$\mathfrak{o}(a)|(i\mathfrak{o}(a^i))$ and so $(\mathfrak{o}(a)/d)|\big((i/d)\mathfrak{o}(a^i)\big)$. Since $\mathfrak{o}(a)/d$ and i/d are relatively prime, it follows that $\mathfrak{o}(a)/d$ divides $\mathfrak{o}(a^i)$. Along with the previous statement, this gives $\mathfrak{o}(a^i)=\mathfrak{o}(a)/d$.

Grading: first and second steps 2pts each; last step 1pt.

Note: the hint on the exam contained a typo, which made it slightly easier to use. Full credit was awarded for the use of either the incorrect statement of the hint or its correct version above.

Problem 4 (2+3+7+3+5pts)

Let $(G,*)$ be a group of order 9 with identity element e. Justify all answers below.

(a) *Let $a\in G$ be any element. What are the possible orders $\mathfrak{o}(a)$ of a and why?*
Since the order $\mathfrak{o}(a)$ divides $|G|=9$ (by Lagrange's Theorem), the only possibilities for $\mathfrak{o}(a)$ are 1,3,9.

Grading: correct answer and some explanation 1pt each

(b) *Suppose G contains an element a with $\mathfrak{o}(a)=9$. Show that $(G,*)$ is isomorphic to $(\mathbb{Z}_9,+)$.*
Let $a\in G$ be such that $\mathfrak{o}(a)=9$. Thus, $a^i=a^j$ if and only if $9|(i-j)$. It follows that the elements $e=a^0, a=a^1, a^2,\ldots,a^8$ of G are all distinct. Since there are 9 of them and $|G|=9$, there are no other elements of G. Thus, G is a cyclic group of order 9 generated by a. Since $(\mathbb{Z}_9,+)$ is a cyclic group generated by $[1]_9$, the two groups are isomorphic. An explicit isomorphism is obtained by sending $a^k\in G$ to $[k]_9\in\mathbb{Z}_9$.

Grading: G is cyclic generated by a 2pts; some connection with $(\mathbb{Z}_9,+)$ 1pt

(c) *Suppose G contains no element a with $\mathfrak{o}(a)=9$. Let $a,b\in G$ be such that $a,b\neq e$ and the cyclic subgroup $\langle a\rangle$ of G generated by a does not contain b. Show that*

$$\mathfrak{o}(a),\mathfrak{o}(b)=3 \qquad \text{and} \qquad G=\{e,a,a^2,b,b^2,ab,a^2b,ab^2,a^2b^2\}.$$

Since $\mathfrak{o}(a),\mathfrak{o}(b)\neq 1,9$, $\mathfrak{o}(a),\mathfrak{o}(b)=3$. Thus, e,a,a^2 are three distinct elements of G, e,b,b^2 are also three distinct elements of G, and $a^3,b^3=e$. By assumption, $b\neq a,a^2$. If $b^2=a,a^2$, then $b=(b^2)^2=a^2,a^4$ contrary to the assumption. Thus, $b^2\neq a,a^2$. Furthermore,

$$\begin{aligned}
ab &\neq e,a,a^2,b,b^2 && \text{b/c} && b\neq a^2,e,a, \quad a\neq e,b;\\
a^2b &\neq e,a,a^2,b,b^2,ab && \text{b/c} && b\neq a,a^2,e, \quad a^2\neq e,b, \quad a\neq e;\\
ab^2 &\neq e,a,a^2,b,b^2,ab,a^2b && \text{b/c} && b^2\neq a^2,e,a, \quad a\neq b^2,e, \quad b\neq e,a;\\
a^2b^2 &\neq e,a,a^2,b,b^2,ab,a^2b,ab^2 && \text{b/c} && b^2\neq a,a^2,e, \quad a^2\neq b^2,e, \quad b\neq a^2,e, \quad a\neq e.
\end{aligned}$$

Thus, $G=\{e,a,a^2,b,b^2,ab,a^2b,ab^2,a^2b^2\}$.

Alternative Solution. Since $\mathfrak{o}(a),\mathfrak{o}(b)\neq 1,9$, $\mathfrak{o}(a),\mathfrak{o}(b)=3$. Thus, e,a,a^2 are three distinct elements of G, e,b,b^2 are also three distinct elements of G, and $a^3,b^3=e$. By assumption, b is not in the subgroup $\langle a\rangle$ of G. Since $b=(b^2)^{-1}$ and $\langle a\rangle$ is closed under inverses, neither is b^2. Thus, the right cosets $\langle a\rangle b$ and $\langle a\rangle b^2$ are different from the right coset $\langle a\rangle e=\langle a\rangle$. Since $\langle a\rangle\neq\langle a\rangle b$, $\langle a\rangle b\neq\langle a\rangle b^2$. Thus, all three right cosets $\langle a\rangle$, $\langle a\rangle b$, and $\langle a\rangle b^2$ are distinct and so disjoint. Since they contain 3 elements each and $|G|=9$, it follows that

$$G=\langle a\rangle\sqcup\langle a\rangle b\sqcup\langle a\rangle b^2=\{e,a,a^2,b,ab,ab^2,b^2,a^2b,a^2b^2\}.$$

Grading: 1pt for first part; content of the rest up to 6pts

(d) *Under the assumptions in (c), show that $ba\neq a^2b^2$. Hint: assume it is and compute $(ab)^2$.*

If $ba=a^2b^2$, then $(ab)^2=a(ba)b=aa^2b^2b=ee=e$. Since $ab\neq e$, it follows that $\mathfrak{o}(a)=2$, which contradicts part (a).

Grading: each of 3 steps 1pt

(e) *Under the assumptions in (c), show that $ba\neq a^2b$. Hint: assume $ba=a^2b$ and compute $(ab)^2$.*

If $ba=a^2b$, then $(ab)^2=a(ba)b=aa^2bb=b^2$ and

$$(ab)^3=(ab)b^2=abb^2=a\neq e.$$

Thus, the order of $\mathfrak{o}(ab)\neq 1,3$, contrary to (c).

Hint: first and last steps 1pt each; middle step up to 3pts

Problem 5 (2+2+6+8pts)

A linear coding function $f\colon \mathbb{Z}_2^3 \longrightarrow \mathbb{Z}_2^6$ *is given by the generator matrix*

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

(a) *What codewords does* f *produce for 000 and 111? Answer only.*

codeword for 000 = 000000	codeword for 111 = 111010

Grading: X wrong answers; each correct answer 1pt

(b) *What words do the codewords 001111 and 111010 stand for? Answer only.*

001111 *stands for* 001	111010 *stands for* 111

Grading: X wrong answers; each correct answer 1pt

(c) *What is the maximum number of errors can this code detect? What is the maximum number of errors can this code correct? Put your answers in the boxes provided and justify them below.*

max to detect = 2	*max to correct* = 1

The minimum weight of each nonzero codeword is 3. This can be seen by computing all 8 codewords, for example. Alternatively, this is immediate for the words of weight 1 because each row has at 3 nonzero entries. It is also immediate the only weight 3, 111, because the first 3 bits of a codeword are the same as the associated word. The codeword of a weight 2 word has two nonzero bits among the first 4 bits and at least another one in the last 3 because the last triples of entries in any pair of rows are distinct. Since the code is linear and the minimum weight of a nonzero codeword is 3, the distance between any two codewords is also 3. Thus, the code can detect $3-1$ errors and correct $(3-1)/2$ errors.

Grading: minimum distance 2pts; explanation 2pts; answers based on the minimum distance or by themselves 1pt each

(d) *The messages received, possibly with errors, are (i) 110111 and (ii) 011100. What words should these messages be decoded to? Put your answers in the boxes provided and justify them below.*

(i) 110	(ii) 011

Multiplying 110111 and 011100 by the detector matrix

$$D = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

we obtain the associated syndromes 010 and 000, respectively. The second implies that 011100 is a codeword, which stands for 011. Since all rows of D are distinct, the first implies that the error occurred in the fifth bit (if there was only one error). Thus, the intended codeword was likely 110101, which stands for 110.

Grading: answers 1pt each; explanation for (i) 4pts and for (ii) 2pts