Math 350: Groups, Rings and Fields
Final Exam (spring 2016)

NAME:

- Attempt problems 1-8. Problems 9 and 10 are optional.
- **Justify all your answers.** (If you are unsure whether or not something requires further justification, you are welcome to ask me.) Please write clearly and legibly, and cross out or erase anything that you do not want graded.
- You may use the course textbook (Ch.0-14, 16-21), your class notes, and old homework and exams. Please clearly identify any theorems or previous results you use.
- No other textbooks, websites, calculators or outside help may be used on this exam.
- All discussion about this exam is strictly prohibited (including conversations about how easy/hard a question is, and how much progress you have made so far).

<table>
<thead>
<tr>
<th>Problem Number</th>
<th>Possible Points</th>
<th>Points Earned</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>3*</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>3*</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100</strong></td>
<td></td>
</tr>
</tbody>
</table>
1. (14 points) Let $\sigma = (2 \ 5 \ 4)(3 \ 7)$ and $\tau = (4 \ 6 \ 5)(1 \ 7 \ 3 \ 2)$ be elements of $S_7$.

(a) Express $\sigma \tau$ as a product of disjoint cycles, and use your answer to find the order of $\sigma \tau$.

\[
\sigma \tau = (2 \ 5 \ 4)(3 \ 7)(4 \ 6 \ 5)(1 \ 7 \ 3 \ 2) = (1 \ 3 \ 5 \ 2)(4 \ 6)
\]

\[
\Rightarrow \quad o(\sigma \tau) = \text{LCM}(4,2) = 4
\]

(b) Express $\sigma \tau$ as a product of transpositions and determine whether it is even or odd.

\[
\sigma \tau = (1 \ 3 \ 5 \ 2)(4 \ 6)
\]

\[
= (1 \ 2)(1 \ 5)(1 \ 3)(4 \ 6) \quad \text{(many other answers are possible)}
\]

4 transpositions $\Rightarrow \sigma \tau$ is an even permutation.

(c) What is the order of the element $A_7 \sigma \ast A_7 \tau$ in the quotient group $S_7/A_7$?

\[
A_7 \sigma \ast A_7 \tau = \left( A_7(\sigma \tau) \right) \quad \text{as} \ \sigma \tau \text{ is even (hence lies in } A_7), \ \text{so } A_7(\sigma \tau) \text{ is the identity in } S_7/A_7
\]

\[
\Rightarrow \quad \text{the order is } [1].
\]

(d) Is there an odd permutation of order 7 in $S_7$? If so, give an example, and if not, explain why.

\[
\text{No. If } \phi \in S_7 \text{ is odd, then } \phi^7 \text{ is also odd, so it cannot be the identity.}
\]
2. (13 points) Let \( R = \mathbb{Z}[\sqrt{3}] = \{ a + b\sqrt{3} \mid a, b \in \mathbb{Z} \} \) and let
\[
S = \left\{ \begin{pmatrix} a & b \\ 3b & a \end{pmatrix} \bigg| a, b \in \mathbb{Z} \right\}.
\]
Show that \( R \) and \( S \) are isomorphic rings.

Define \( \varphi : R \rightarrow S \) by
\[
\varphi(a + b\sqrt{3}) = \begin{pmatrix} a & b \\ 3b & a \end{pmatrix}.
\]

Then
\[
\varphi((a_1 + b_1\sqrt{3}) + (a_2 + b_2\sqrt{3})) = \varphi((a_1 + a_2) + (b_1 + b_2)\sqrt{3})
= \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ 3(b_1 + b_2) & a_1 + a_2 \end{pmatrix}
= \begin{pmatrix} a_1 & b_1 \\ 3b_1 & a_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ 3b_2 & a_2 \end{pmatrix}
= \varphi(a_1 + b_1\sqrt{3}) + \varphi(a_2 + b_2\sqrt{3})
\]

\& \ \varphi((a_1 + b_1\sqrt{3})(a_2 + b_2\sqrt{3})) = \varphi((a_1 a_2 + 3b_1 b_2) + (a_1 b_2 + a_2 b_1)\sqrt{3})
= \begin{pmatrix} a_1 a_2 + 3b_1 b_2 & a_1 b_2 + a_2 b_1 \\ 3(b_1 a_2 + a_1 b_2) & a_1 a_2 + 3b_1 b_2 \end{pmatrix}
= \begin{pmatrix} a_1 & b_1 \\ 3b_1 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 3b_2 & a_2 \end{pmatrix}
= \varphi(a_1 + b_1\sqrt{3}) \varphi(a_2 + b_2\sqrt{3})
\]

So \( \varphi \) is a ring homomorphism.

\( \varphi \) is bijective, since (for example) it has inverse function
\[
\psi \left( \begin{pmatrix} a & b \\ 3b & a \end{pmatrix} \right) = a + b\sqrt{3}.
\]

So \( \varphi \) is an isomorphism, hence \( R \cong S \).
3. (13 points) Let $G$ be the set of all $2 \times 2$ matrices with real number entries. Then $G$ is a group under the operation of matrix addition. Let

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \bigg| a + d = 0 \right\}.$$ 

Show that $G/H$ and $(\mathbb{R}, +)$ are isomorphic groups.

Define

$$\varphi : G \rightarrow \mathbb{R}$$

by

$$\varphi \left( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) = a + d.$$ 

$\varphi$ is a group hom. (for $(G, +)$ & $(\mathbb{R}, +)$), since

$$\varphi \left( \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \right) = \varphi \left( \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix} \right) = a_1 + a_2 + d_1 + d_2$$

$$= (a_1 + d_1) + (a_2 + d_2) = \varphi \left( \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \right) + \varphi \left( \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \right).$$

$\varphi$ is surjective, since $\forall a \in \mathbb{R}, a = \varphi \left( \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right)$ (for example).

$$\ker \varphi = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a + d = 0 \right\} = H.$$ 

So by the fund. thm of group homomorphisms,

$$G/H \cong \mathbb{R}.$$
4. (10 points) Let \( \varphi : R \to T \) be a ring homomorphism that is onto, and let \( I \) be an ideal of \( R \). Show that \( \varphi(I) \) is an ideal of \( T \), where \( \varphi(I) = \{ \varphi(a) \mid a \in I \} \).

(This theorem is stated in the book, but it is stated without proof. You are required to explicitly prove all necessary parts of this here, instead of citing the theorem.)

It suffices to check that \( \varphi(I) \) is nonempty, closed under subtraction and sticky.

\( \varnothing \in I \Rightarrow \varphi(\varnothing) \in \varphi(I) \), so \( \varphi(I) \) is nonempty.

\( \forall x, y \in \varphi(I) \), \( \exists a, b \in I \) s.t. \( x = \varphi(a) \) & \( y = \varphi(b) \).

so \( x - y = \varphi(a) - \varphi(b) = \varphi(a - b) \)

\& \( a - b \in I \) (\( I \) is closed under subtraction).

hence \( x - y \in \varphi(I) \); \( \varphi(I) \) is closed under subtraction.

\( \forall x \in \varphi(I) \) and \( s \in S \),

\( \exists a \in I \) s.t. \( \varphi(a) = x \), \( \& \exists r \in R \) s.t. \( \varphi(r) = s \) (\( \varphi \) is surjective).

\( \Rightarrow xs = \varphi(a) \varphi(r) = \varphi(ar) \) \& \( ar \in I \) (\( I \) is sticky).

\( \Rightarrow xs \in \varphi(I) \)

\& similarly \( sx = \varphi(ra) \in \varphi(I) \).

So \( \varphi(I) \) is sticky.

Hence \( \varphi(I) \) is an ideal.
5. (14 points) Define a relation \( R \) on the set \( M_{2 \times 2}(\mathbb{R}) \) of \( 2 \times 2 \) real matrices by \( A R B \) for \( A, B \in M_{2 \times 2}(\mathbb{R}) \) if and only if there exists an invertible matrix \( P \in \text{GL}(2, \mathbb{R}) \) such that \( A = PB \).

(a) Show that \( R \) is an equivalence relation on \( M_{2 \times 2}(\mathbb{R}) \).

Reflexivity:
\[ \forall A \in M_{2 \times 2}(\mathbb{R}), \quad A = I_2 A \quad \text{(where } I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}) \],
so \( A RA \) (I is invertible).

Symmetry:
If \( A RB \), then \( \exists \) an invertible matrix \( P \) st.
\[ A = PB. \]

So \( P^{-1}A = P^{-1}PB = IB = B. \)
\( P^{-1} \) is also invertible, hence \( B = P^{-1}A \Rightarrow RB \). So \( R \) is symmetric.

Transitivity:
If \( A RB \) \& \( B RC \), then \( \exists \) invertible matrices \( P, Q \) st.
\[ A = PB \quad \& \quad B = QC \]

\[ \Rightarrow A = (PB)C = PBC. \]

\( PQ \) is invertible (its inverse is \( Q^{-1}P^{-1} \)), so \( A RC \). So \( R \) is transitive.

(b) What are the equivalence classes of the identity matrix \( I_2 \) and the zero matrix \( O_2 \)? (Note that these two sets will have orders.)

\( ARI_2 \) iff \( A = P I_2 = P \) for an invertible matrix \( P \)

iff \( A \) is invertible.

So the class of \( I_2 \) is \( \text{GL}_2(\mathbb{R}) \) (the set of invertible matrices).

\( ARO_2 \) iff \( A = P O_2 = O_2 \) for some inv \( P \)

iff \( A = O_2 \).

So the class of \( O_2 \) contains only \( O_2 \); it is \{ \( O_2 \} \).
6. (14 points) Let $F = \mathbb{Z}_7$ and $R = F[X]$.

(a) What are the zero divisors in $R$?

$f(x)g(x) = 0_F$ if and only if $\deg[f(x)] + \deg[g(x)] = -\infty$

iff $\deg f(x) + \deg g(x) = -\infty$

iff $\deg f(x) = -\infty$ or $\deg g(x) = -\infty$

iff $f(x) = 0_F$ or $g(x) = 0_F$.

So the only zero divisor is $0_F$ itself.

(b) What are the units in $R$?

$R^\times = F^\times$ (as shown on Page 11).

Any $u \in F^\times$ is a unit since $u \in F$, and no non-constant $f(x)$ is a unit since $1_F = f(x)q(x) \Rightarrow \deg f(x) + \deg q(x) = 0 \Rightarrow \deg f(x) = \deg q(x) = 0$.

(c) Let $f(X) = X^2 + 5$ and let $I = (f(X))$. How many elements are in $R/I$?

$R/I \cong \mathbb{Z}_7[X]/(X^2 + 5)$, where $r(x)$ is the remainder when $r(x)$ is divided by $x^2 + 5$; $\deg r(x) \leq 2$.

So any elt of $R/I$ is $ax + b$ for some $a, b \in \mathbb{Z}_7$.

No two such els are equal, since all monomials of $x^2$ have degree $\geq 2$.

So $|R/I| = |\mathbb{Z}_7| \cdot |\mathbb{Z}_7| = 49$.

(d) Is $R/I$ a field? Justify your answer.

No; $X^2 + 5$ has a root in $F$: $3^2 + 5 = 2 + 5 = 0$ (in $F = \mathbb{Z}_7$).

$\Rightarrow X^2 + 5$ is reducible $\Rightarrow (X^2 + 5)$ is not maximal $\Rightarrow R/I$ is not a field.

Specifically, $X^2 + 5 = (X + 3)(X + 4)$

(e) Is $R/I$ a domain? Justify your answer.

No: $X + 3 \neq 0$, but

$X + 4 \cdot X + 3 = X^2 + 4 = 0$. 

7
7. (12 points) Write down the orders of the following groups:

(a) The group of $5 \times 5$ permutation matrices with determinant 1. (Recall that a permutation matrix is a matrix with a single entry equal to 1 in every row and column, and 0 everywhere else.)

(b) $D_4/Z(D_4)$, where $Z(D_4)$ is the center of $D_4$.

Write $D_4 = \{e, f, f^2, f^3, g, gf, gf^2, gf^3\}$ as in class.

One can check that $e, f^2$ commute with everything, but no other elements do.

$\Rightarrow \ Z(D_4) = \{e, f^2\} \Rightarrow |Z(D_4)| = 2 \Rightarrow |D_4/Z(D_4)| = \frac{8}{2} = 4$

(c) $\langle x^6 \rangle$, where $o(x) = 10$

$$o(x^6) = \frac{10}{\gcd(10, 6)} = \frac{10}{2} = 5$$

(d) $G/H$ where $G = \mathbb{Z}_{15} \times \mathbb{Z}_4$ and $H = \langle (5, 2) \rangle$

$$o((5, 2)) = \text{LCM}(o(5) \text{ in } \mathbb{Z}_{15}, o(2) \text{ in } \mathbb{Z}_4)$$

$$= \text{LCM}(3, 2) = 6$$

$\Rightarrow \ |H| = 6$.

Since $|G| = |\mathbb{Z}_{15}| \cdot |\mathbb{Z}_4| = 60$, it follows that

$$|G/H| = \frac{|G|}{|H|} = \frac{60}{6} = 10$$
8. (10 points) Let $G$ be a group and $H \triangleleft G$.

(a) Show that if $x \in G$ is an element such that $o(x) = m$, then $o(Hx)$ is finite in $G/H$ and divides $m$.

\[ x^m = e_G \text{ since } o(x) = m, \]
\[ \Rightarrow (Hx)^m = Hx^m = H e_G = e_{G/H}, \]
\[ \Rightarrow o(Hx) \mid m \quad \text{(in particular, } o(Hx) \text{ is finite)}.\]

(b) Show that if $|G/H| = n$, then $g^n \in H$ for all $g \in G$. (Note that this part is completely independent from part (a).)

By Lagrange's theorem, \( \forall g \in G, \quad (Hg)^{\frac{|G/H|}{n}} = e_{G/H} \)
\[ \Rightarrow (Hg)^{n} = H e_{G/H} \]
\[ \Rightarrow H g^n = H e_{G/H} \]
\[ \Rightarrow g^n \in H. \]
9. **Optional Bonus Problem:** (3 points) We know that $\mathbb{Z}_{6011}^\times$ is a group under $\circ$ (i.e., multiplication mod 6011), since 6011 is a prime number. Find the inverse of 1001 in $(\mathbb{Z}_{6011}^\times, \circ)$. (Your answer should be an explicit integer between 0 and 6010. Note that this can be computed without a calculator.)

Note: this is trickly if you haven't studied the Euclidean algorithm in Sec (which we didn't discuss in class).

$$6 \cdot 1001 = 6006 \equiv -5 \mod 6011$$

mul. by 200:

$$\Rightarrow 1200 \cdot 1001 \equiv -1000 \mod 6011$$

add 1001:

$$\Rightarrow 1201 \cdot 1001 \equiv 1 \mod 6011$$

So $1001^{-1} = 1201$ in $\mathbb{Z}_{6011}$.
10. **Optional Bonus Problem:** (3 points) Give an example of a group $G$ and elements $x, y \in G$ such that $o(x) = o(y) = 2$, but $o(xy)$ is infinite.

Note: in any such example, $G$ must be non-abelian, & infinite.

Here are a couple examples:

1) $G = \text{Sier}$, bijections $\mathbb{R} \rightarrow \mathbb{R}$.

- $f \in G$ defined by $f(x) = -x$.
- $g \in G$ defined by $g(x) = 1 - x$.

Then $f \circ f(x) = -(-x) = x$ & $g \circ g(x) = 1 - (1 - x) = x$.

So both $f$ & $g$ have order 2.

- $f \circ g(x) = -(1 - x) = x - 1$.

So $(f \circ g)^n(x) = x - n \neq x$, $\forall n \geq 1$.

$\Rightarrow o(f \circ g) = \infty$.

2) $G = \text{GL}(2, \mathbb{R})$. Let $A \in G$ be $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ & $B \in G$ be the matrix rep. of reflection across a line making angle $\theta$ with the x-axis. One can check that $BA$ represents a transformation that rotates the plane by $2\theta$, counterclockwise. So as long as $\theta / \pi \notin \mathbb{Q}$, no power $(BA)^n$ is the identity (except $n=0$), i.e. $o(BA) = \infty$. But $A^2 = B^2 = I$. 

11