Math 347, H/wk 11 (Solutions)  
Due Wednesday, April 17

PRINT YOUR NAME:

**Problem 1.** Consider the matrix $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in GL(2, \mathbb{R})$. Find the order $ord(A)$ of $A$ in $GL(2, \mathbb{R})$.

**Solution.**  
A direct computation shows that for every $n \in \mathbb{N}$ we have  
$$A^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$$  
Thus there does not exist $n \in \mathbb{N}$ such that $A^n = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Therefore, by definition of the order of an element in a groups, we have $ord(A) = \infty$ in $GL(2, \mathbb{R})$.

**Problem 2.**  
Let $n \geq 2$ be an integer and consider the $n$-cycle $\sigma = (1 \ 2 \ 3 \ \cdots \ n) \in S_n$.

**Solution.**  
A direct computation shows that for $i = 1, 2, \ldots, n-1$ we have $\sigma^i(1) = i$ and that $\sigma^n(1) = 1$.  
Thus for $1 \leq i \leq n-1$ we have $\sigma^i(1) \neq 1$ and hence $\sigma^i \neq Id_{\{1, 2, \ldots, n\}}$.  
Hence $ord(\sigma) > n-1$.

As we observed above, $\sigma^n(1) = 1$. For each $j \in \{1, 2, \ldots, n\}$ we can also write $\sigma$ as $\sigma = (j \ j+1 \ \cdots \ n \ 1 \ 2 \ \cdots \ j-1)$. Then the same argument used to show that $\sigma^n(1) = 1$ also shows that $\sigma^n(j) = j$ for every $j \in \{1, 2, \ldots, n\}$.

Thus $\sigma^n = Id_{\{1, 2, \ldots, n\}}$ and hence $ord(\sigma) \leq n$. Since we already know that $ord(\sigma) > n-1$, it follows that $ord(\sigma) = n$.

**Problem 3.**  
Let $G$ be a group, let $g \in G$ be such that $1 \leq ord(g) < \infty$. Denote $m = ord(g)$.

(1) Prove that $g^i \neq g^j$ wherever $i, j \in \{0, 1, \ldots, m-1\}$ and $i \neq j$.

(2) Prove that for $n \in \mathbb{Z}$ we have $g^n = e$ if and only if $m|n$.

**Proof.**  
(1) Suppose, on the contrary, that there exist $i, j \in \{0, 1, \ldots, m-1\}$ such that $i \neq j$ but $g^i = g^j$. Then either $i < j$ or $j < i$. Without loss of generality we may assume that $i < j$.

Then from $g^i = g^j$ we get  
$$1 = g^{-i}g^i = g^{-i}g^j = g^{j-i}$$  
We have $0 < j-i < m$, so that $j-i \in \{1, \ldots, m-1\}$. The fact that $g^{j-i} = 1$ and that $1 \leq j-i < m$ now contradicts the fact that $ord(g) = m$, so that
$m$ is the smallest $n \in \mathbb{N}$ such that $g^n = 1$. This contradiction shows that our assumption that there exist $i, j \in \{0, 1, \ldots, m - 1\}$ such that $i \neq j$ but $g^i = g^j$ was false. Hence if $i, j \in \{0, 1, \ldots, m - 1\}$ and $i \neq j$ then $g^i \neq g^j$, as required.

(2) Suppose first that $m \mid n$, so that $n = km$ for some $k \in \mathbb{Z}$. Then $g^n = g^{mk} = (g^m)^k = 1^k = 1$, as required.

Suppose now that $n \in \mathbb{Z}$ is such that $g^n = 1$. We divide $n$ with the remainder by $m$ and get $n = qm + r$ where $q, r \in \mathbb{Z}$ and $0 \leq q \leq m - 1$.

Then

$$g^q = g^{n-mq} = g^n g^{-mq} = g^n(g^m)^{-q} = 1 \cdot 1^{-q} = 1.$$ 

Thus $g^q = 1$ and $q \in \{0, 1, \ldots, m - 1\}$. By definition of the order of an element, the fact that $m = \text{ord}(g)$ now implies that $q = 0$. Thus $n = qm$, so that $m \mid n$, as required.

Problem 4.

Prove that if $G$ is a finite group and $g \in G$ then $\text{ord}(g) < \infty$.

Proof. Consider the elements

$$g, g^2, g^3, \ldots, g^n, \ldots.$$ 

Since $G$ is a finite set the above list must contain repetitions, and hence there exist $i, j \in \mathbb{N}$ such that $i < j$ but $g^i = g^j$. Therefore

$$1 = g^{-i}g^i = g^{-i}g^j = g^{j-i}.$$ 

Thus $j - i \in \mathbb{N}$ and $g^{j-i} = 1$. Hence $S := \{n \in \mathbb{N} : g^n = 1\} = \neq \emptyset$ and hence $\text{ord}(S) = \min\{n : n \in S\} < \infty$.

Problem 5.

Let $G$ and $H$ be two finite groups and consider their direct product group $(G \times H, \cdot)$, with the binary operation $\cdot$ on $G \times H$ defined as $(g, h) \cdot (g', h') = (gg', hh')$, where $g, g' \in G$ and $h, h' \in H$. (You do not have to prove that $(G \times H, \cdot)$ is a group.)

Let $g \in G$ and $h \in H$ and let $m = \text{ord}(g)$ and $n = \text{ord}(h)$. Put $a = (g, h) \in G \times H$.

Prove that $\text{ord}(a) = \text{lcm}(m, n)$.

Proof. Recall that the identity element in $G \times H$ is $(1_G, 1_H)$, where $1_G \in G$ is the identity element in $G$ and where $1_H \in H$ is the identity element in $H$.

Put $k = \text{lcm}(m, n)$. Thus $k = mq = nt$ for some $q, t \in \mathbb{Z}$. Therefore

$$a^k = (g, h)^k = (g^k, h^k) = (g^{mq}, h^{nt}) = ((g^m)^q, (h^n)^t) = (1_G^q, 1_H^t) = (1_G, 1_H).$$ 

Suppose now that $s \in \mathbb{N}$ is such that $a^s = (1_G, 1_H)$. Thus

$$(1_G, 1_H) = a^s = (g^s, h^s)$$.
so that \( g^s = 1_G \) and \( h^s = 1_H \). By the result of Problem 3 applied to \( G \) and \( H \), it follows that \( \text{ord}(g)|s \) and \( \text{ord}(h)|s \), that is \( m|s \) and \( n|s \). Hence \( s \in \mathbb{N} \) is a common multiple of \( m, m \) and hence \( k = \text{lcm}(m, n) \leq s \).

Thus we see that \( a^k = (1_G, 1_H) \) and that if \( s \in \mathbb{N} \) is such that \( a^s = (1_G, 1_H) \) then \( k \leq s \). Hence, by definition of the order of an element, we get \( \text{ord}(a) = k \), that is \( \text{ord}(k) = \text{lcm}(m, n) \), as required.

\[ \square \]

**Problem 6.**

Let \( G = S_5 \), \( g = (1 \ 3 \ 2 \ 4) \in S_5 \) and \( H = \langle g \rangle \). Find the index \([G : H]\) of \( H \) in \( G \).

**Solution.**

By Problem 2 above we know that \( \text{ord}(g) = 4 \). Hence, by a Theorem stated in class, 
\[
4 = \text{ord}(g) = |\langle g \rangle| = |H|.
\]

By Lagrange’s Theorem we have
\[
[G : H] = \frac{|G|}{|H|} = \frac{5!}{4} = \frac{120}{4} = 30.
\]

**Problem 7.**

Let \( G = GL(2, \mathbb{R}) \) and \( H = SL(2, \mathbb{R}) \leq G \). Let \( g = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \in GL(2, \mathbb{R}) \).

1. Prove that if \( m, n \in \mathbb{Z} \) and \( m \neq n \) then \( g^nH \neq g^mH \).

2. Prove that \([G : H] = \infty\).

**Proof.** A direct computation shows that for all \( n \in \mathbb{Z} \)
\[
g^n = \begin{bmatrix} 2^n & 0 \\ 0 & 1 \end{bmatrix}.
\]

We claim that if \( m, n \in \mathbb{Z} \) and \( m \neq n \) then \( g^nH \neq g^mH \). Indeed, suppose not, so that there exist \( m, n \in \mathbb{Z} \) such that \( m \neq n \) and \( g^nH = g^mH \). Then \( g^n = g^m h \) for some \( h \in H = SL(2, \mathbb{R}) \). Hence \( g^{m-n} = g^{-m}g^n = h \in H = SL(2, \mathbb{R}) \). However, \( g^{m-n} = \begin{bmatrix} 2^{m-n} & 0 \\ 0 & 1 \end{bmatrix} \). Therefore we have \( \det(g^{m-n}) = 2^{m-n} \neq 1 \), since \( m \neq 1 \). This contradicts the fact that \( g^{m-n} = h \in H = SL(2, \mathbb{R}) \).

(2) By (1) we know that the cosets
\[
1H, gH, g^2H, \ldots, g^nH, \ldots,
\]
are pairwise distinct elements of \( G/H \). Hence the set
\[
G/H = \{ aH | a \in G \}
\]
is infinite. Therefore, by definition of the index of a subgroup, we have
\[
\]
\[ \square \]