Midterm

The grader cannot be expected to work his way through a sprawling mess of identities presented without a coherent narrative through line. If he can’t make sense of it in finite time you could lose coherent narrative through line. If he can’t make sense of it in finite time you could lose serious points. Coherent, readable exposition of your work is half the job in mathematics.

Problem 1 :
Consider a composite \( \phi \circ \psi(x) = \phi(\psi(x)) \) of two maps \( X \xrightarrow{\psi} Y \xrightarrow{\phi} Z \). If the maps \( \phi \) and \( \psi \) are injective/surjective/bijective, what can you say about \( \phi \circ \psi \)? Write \( I \) if the composite is injective but not surjective , \( S \) if it is subjective but not one-to-one, and \( B \) if is bijective. (These possibilities are mutually exclusive.)

1. Enter one of these symbols in the following diagram if the composite \( \phi \circ \psi \) always has that property.

2. Write \( \times \) if \( \phi \circ \psi \) does not always have one of these properties.

\[
\begin{array}{ccc}
\text{map } \phi \\
I & S & B \\
\hline \\
\text{map } \psi \\
I \\
S \\
B \\
\end{array}
\]

You need not give any explanation for your answers, but will lose points for incorrect answer.

Solution :

\[
\begin{array}{ccc}
\text{map } \phi \\
I & S & B \\
\hline \\
\text{map } \psi \\
I & \times & I \\
S & \times & S \\
B & I & S & B \\
\end{array}
\]

Problem 2 :
The rational numbers \( \mathbb{Q} \) are constructed from the integers \( \mathbb{Z} \) by imposing
an RST relation \( \sim \) on the set of pairs of elements of \( \mathbb{Z} \),

\[
X = \{(p,q) : p, q \in \mathbb{Z}, q \neq 0\} : \\
(p,q) \sim (r,s) \iff ps = qr
\]

Then \( Q \) is the space of equivalence classes \([[(p,q)]]\) of fraction symbols. We impose algebraic operation \((+\)) and \((\cdot)\) in \( Q \) by defining

\[
[(p,q)] + [(r,s)] = [(pq + qr,qs)] \text{ and } [(p,q)] \cdot [(r,s)] = [(pr,qs)]
\]

From these definitions, prove that these operations well defined in spite of our use of representatives in their definitions, that means prove that \((p,q) \sim (p',q')\) and \((r,s) \sim (r',s')\) implies that \( (p + qr,qs) \sim (p' + q'r', q's') \) and \( (pr,qs) \sim (p'r', q's') \). (Note: We denote \( p \{q = \{rp,qs\} \).)

**Solution:**

Following the hint, try the second identity first:

Data : \( (p,q) \sim (p',q') \) so \( pq' = p'q \) in \( \mathbb{Z} \), \( (r,s) \sim (r',s') \) so \( rs' = r's \). To be proven : \( (pr,qs) \sim (p'r', q's') \), or \( prq's' = p'r'qs \) in \( \mathbb{Z} \). Substitute \( rs' = r's \) to make this \( p'q'r's = p'r'qs = ( \text{right side of } (1) ) \). Done.

For \((a)\), we have same data and must show :

\[
(ps + qr)q's' = psq's' + qrq's'
\]

is equal to \( qs(p's' + q'r') = qsp's' + qsq's' \). On then left, make substitutions

\[
psq's' + qrq's' = p'qss' + qrq's' = p'qss' + qq'r's
\]

This is equal to the right side, as desired.

**Problem 3:**

Let \((G,+)\) be an abelian group written in the additive notation. Integer \( k \in \mathbb{Z} \) act on group element \( x \in G \) by taking additive powers

\[
\begin{align*}
k \cdot x &= x + \cdots + x \quad (k \text{ times if } k > 0) \\
0 \cdot x &= 0_G \\
-k \cdot x &= (-x) + \cdots + (-x) \quad (k > 0; -x \text{ is additive inverse of } x)
\end{align*}
\]

If \( a,b \in G \), prove that

1. The subset \( S = \mathbb{Z}a + \mathbb{Z}b = \{k \cdot a + l \cdot b : k,l \in \mathbb{Z}\} \) is a subgroup of \( (G,+); \)

2. \( S \) is precisely the subgroup \( H = \langle a,b \rangle \) generated by \( a \) and \( b \).

**Solution:**

1. We must show

   (a) \( 0 = 0_E \in S \);
(b) $S + S \subseteq S$;

(c) the set of additive inverses $-S$ is $\subseteq S$. Since $0 \cdot a = 0_G$, $0 \cdot b = 0_G$ and $0_G + 0_G = 0_G$ we get $0_G \in S$.

For 3,

$$\begin{align*}
(k \cdot a + l \cdot b) + (k' \cdot a + l' \cdot b) &= k \cdot a + k' \cdot a + l \cdot b + l' \cdot b \\
&= (k + k') \cdot a + (l + l') \cdot b
\end{align*}$$

(commutativity, associativity of (+) operation)

(Exponent laws)

So, $S + S \subseteq S$.

For 3., we know $-(k \cdot x) = (-k) \cdot x = k \cdot (-x)$ by definition of additive $k^{th}$ powers when the exponent is $< 0$. (As a check: $k \cdot x + (-k) \cdot x = (k + (-k)) \cdot x = 0 \cdot x = 0_G$, so $(-k) \cdot x = 0_G$; similarly, $k \cdot x + k \cdot (-x) = 0_G$ so $k \cdot (-x) = -(k \cdot x)$ too.) Thus

$$-(k \cdot a + l \cdot b) = -(k \cdot a) + (-(l \cdot b)) = (-k) \cdot a + (-l) \cdot b$$

is in $S$. $H$ is a subgroup that contains $a, b$.

2. The last remark implies $<a, b> = $ smallest subgroup containing $a, b \subseteq H$. But every $x \in <a, b>$ has the form $x = x_1 + \cdots + x_m$ ($m < \infty$) where $x_i = \pm a$ or $\pm b$.

Since $G$ is abelian we may gather together all occurrences of $\neq a$ followed by the

$x_i \neq \pm b$ to rewrite this word as $n_1 a + (-n_2) a + n_3 b + (-n_4) b$ ($n_1 = n_2 + n_3 + n_4 = m$, $n_i > 0) = (n_1 - n_2) \cdot a + (n_3 - n_4) \cdot b$. This lies in $H$, so $x \in <a, b> \Rightarrow x \in H$ and $<a, b> \subseteq H$. Hence $<a, b> = H$.

**Problem 4:**

Let $H$ be a subgroup in a finite group $G$. If $G$ is generated by a set $S$, so $G = <S>$, prove that $H$ is a normal subgroup in $G$ if and only if $sHs^{-1} \subseteq H$ for all $s \in S$.

**Note:** Results of this sort are useful because it is easier to check an algebraic property for a small set of generators than to prove it holds for all elements of $G$.

**Solution:**

If $G = <S>$, $H$ a subgroup and $sHs^{-1} = H$ for all $s \in S$ first observe that $Hs^{-1} = s^{-1}H$ and $H = s^{-1}Hs$ for all $s \in S$, so $H$ is invariant under conjugation by every element $m$ the enlarged "alphabet" $SU$S$^{-1}$. $G$ then consists of all "words" of finite length:

1. $w = w_1 \ldots w_r$ such that $r < w$, each $w_i \in S \cap S^{-1}$. We must show $wHw^{-1} = H$ for all such $w$. But if $h \in H$,

$$wHw^{-1} = (w_1 \ldots w_r)H(w_1 \ldots w_r)^{-1} = (w_1 \ldots w_r)H(w_r^{-1} \ldots w_1^{-1}) = w_1(w_2(\ldots (w_rHw_r^{-1}) \ldots w_2^{-1})w_1^{-1})$$

But $w_iHw_i^{-1} = H$, for any $w_i \in S \cap S^{-1}$ so $w_rHw_r^{-1} = H$, $w_r^{-2}w_{r-1}Hw_{r-1}^{-1}w_{r-2}^{-1} = w_r^{-2}Hw_{r-2}^{-1}$, etc. We conclude that $wHw^{-1} \in H$ for all words, so $H$ is normal in $G$. 

3.
Problem 5:
If \( G \) is a group that has no proper subgroups (\( H \neq \{e\} \) and \( H \neq G \)), In this exercise we will prove that:

1. \( G \) must be cyclic and finite.
2. Either \( G \) is trivial or \( G \cong (\mathbb{Z}/p\mathbb{Z},+) \) for some prime \( p > 1 \).

We do not assume \( G \) finite.

In order to prove this, please follow the questions above:

1. If \( G \) is non-cyclic, give a proper subgroup of \( G \);
2. If \( G \) is cyclic and of infinite cardinality, to which well-known group \( G \) is it isomorphic (Theorem of structure of cyclic groups)? Give then a proper subgroup of this very well-known group.

We have now proven that \( G \) without proper subgroup implies that it is finite and cyclic.

3. Suppose that \( G \) is finite, cyclic and non-trivial, to which well-known group \( G \) is it isomorphic (Theorem of structure of cyclic groups)? If its cardinality is not prime, find a proper subgroup of this well-known group \( G \).

(Note that this complete the proof).

Solution:

1. If \( a \neq e \) then \( H = \langle a \rangle = \{a^k : k \in \mathbb{Z}\} \) must equal \( G \) if there are no proper subgroups, so \( G \) is cyclic. In notes, we showed \( G \cong \langle \mathbb{Z},+ \rangle \) if \( |G| = \infty \), but \( \mathbb{Z} \) contains proper subgroups such as \( 2\mathbb{Z} \subseteq \mathbb{Z} \), so \( G \) in fact is finite and \( \cong \langle \mathbb{Z}/n\mathbb{Z},+ \rangle \) for some \( n \).

2. We showed that the cyclic generators of the additive group \( \mathbb{Z}/n\mathbb{Z} \) are precisely its units \( U_n = \{[k] : 1 \leq k < n, \gcd(k,n) = 1\} \). If \( n = p \) is a prime its divisors are only \( \pm 1, \pm p \), so \( \gcd(k,p) = 1 \), for all \( 1 \leq k < n \). In this case, \( U_p = \langle \mathbb{Z}/p\mathbb{Z},+ \rangle = \{g \in \mathbb{Z}/p\mathbb{Z} : g \neq [0]\} \) and all \([k] \neq [0]\) generate the entire group \( \langle \mathbb{Z}/p\mathbb{Z},+ \rangle \). Thus if \([k] \neq [0]\) we have \( \langle [k] \rangle = \mathbb{Z}/p\mathbb{Z} \) and there are no proper subgroups. If \( n \) is not a prime, \( n = uv \) with \( 0 < u,v < n \). Then \( k = n/u = v \) is an integer, \( 1 < k < n \), such that \([0],[k],2[k],\ldots,(n/k-1)[k]\) are distinct elements in \([1,n-1]\) and \((n/k)[k] = [n] = [0]\) (Distinct because all the terms \( jk \) are \( < n \) and increase strictly from zero).

Thus \( o([k]) = n/k < n \) and \( H = \langle [k] \rangle = \{j[k] : j \in \mathbb{Z}\} \) has \( |H| = n/k < n = |G| \). But \( |H| > 1 \) because \( k > 1 \), so \( H \) is a proper subgroup.