Solutions to the Midterm

Problem 1. Indicate in your bluebook whether each of the following statements is true or false. No reasoning or proof is required for this question. However, you will lose 1 point for each incorrect answer (each correct answer will gain you 1 point).

(a) A subgroup of a finitely generated group is finitely generated.

This is false. See problem 1 from homework 3 for an example.

(b) A group of order 240 must have a subgroup of order 16.

This is true: $16 = 2^4$ and $240 = 2^4 \cdot 3 \cdot 5$ so any Sylow 2-subgroup of a group of order 240 has order 16.

(c) There exists a non-abelian simple group generated by 2 elements of order 2.

This is false: by part d) of Problem 4 from homework 1 any non-abelian group generated by two elements of order 2 is dihedral and dihedral groups are not simple.

(d) There is a group G such that $[G : Z(G)] = 15$ ($Z(G)$ is the center of G).

This is false: any group order 15 is cyclic (by the description of all groups of order pq where p, q are primes). But if $G/Z(G)$ is cyclic then G is abelian and $G = Z(G)$.

(e) Every abelian group of order 70 is cyclic.

This is true: a finite abelian group G of order n has unique invariant factors decomposition $G = \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$, where $1 < n_1|n_2|\ldots|n_k$ and $n_1 n_2 \ldots n_k = n$. The only possibility when $n = 70 = 2\cdot5\cdot7$ is $k = 1$ and $n_1 = n = 70$.

(f) A subgroup of a finitely generated abelian group is finitely generated.

This is true.

(g) A group of order 81 can act on a set with 2024 elements so that there is exactly 1 fixed point.

This is false: $81 = 3^4$ is a power of the prime 3, so our group is a 3-group. If a p-group acts on a set of size N then the number of fixed points f is such that p divides $N - f$. Since 3 does not divide $2024 - 1 = 2023$, so f can not be 1.

(h) S_6 has an element of order 12.

This is false: the order of a permutation is the least common multiple of the lengths of the cycles in the decomposition of the permutation as a product of disjoint cycles.

To get order 12 we would need a cycle of length divisible by 3 and a cycle of length divisible by 4. Since both $3+4$ and $3 \cdot 4$ are bigger than 6, this is not possible in S_6.

(i) If H is a subgroup of finite index of G and A is a subgroup of G then $A \cap H$ is of finite index in A.

This is true: see part c) of Problem 2 in homework 1.

(j) The group $SL_2(\mathbb{Z})$ is perfect.

This is false: in problem 2 of part 2 of homework 2 it was observed that $SL_2(\mathbb{Z})$ has a normal subgroup K such that the quotient $SL_2(\mathbb{Z})/K$ is isomorphic to the dihedral group of order 6. A dihedral group is not perfect and a quotient of a perfect group is perfect, so $SL_2(\mathbb{Z})$ is not perfect.

Problem 2. a) State Sylow's Theorem. (3 points)

b) Prove that a finite group of order 4225 is abelian. (6 points)

c) List all groups of order 4225 (up to isomorphism). (4 points)

Solution: a) **Sylow Theorem.** Let G be a finite group of order $|G| = p^n m$, where p is a prime, $n \geq 1$ and p does not divide m. Then:

- G has at least one subgroup of order p^n. Any such subgroup is calle a Sylow p-subgroup of G.
- any two Sylow p-subgroups are conjugate in G.
- the number t_p of Sylow p-subgroups divides m and $p|(t_p - 1)$.
- every p-subgroup of G is contained in a Sylow p-subgroup.

b) Note that $4225 = 5^2 \cdot 13^2$. Let G be a group of order 4225. The number t_5 of Sylow 5-subgroups in G divides 13^2, so it can be $1, 13, 169$. Since 5 divides $t_5 - 1$, the only possibility is $t_5 = 1$. This means that G has a normal Sylow 5-subgroup A. Since A has order 5^2, A is abelian (any group of order p^2, p a prime, is abelian).

Similarly, the number t_{13} of Sylow 13-subgroups in G divides 5^2, so it can be $1, 5, 25$. Since 13 divides $t_{13} - 1$, the only possibility is $t_{13} = 1$. This means that G has a normal Sylow 13-subgroup B. Since B has order 13^2, B is abelian.

We see that G has abelian normal subgroups A, B of order 5^2 and 13^2 respectively. Clearly $A \cap B = \{e\}$, so $|AB| = |A||B| = |G|$, i.e. $G = AB$. This implies that $G = A \times B$. A product of abelian groups is abelian, so G is abelian.

c) The group A in part b) is abelian of order 5^2, so it is either $\mathbb{Z}/25\mathbb{Z}$ or $\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$. Similarly, the group B in part b) is abelian of order 13^2, so it is either $\mathbb{Z}/169\mathbb{Z}$ or $\mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$. Thus we have 4 possibilities for $G = A \times B$:

$$\mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/169\mathbb{Z} = \mathbb{Z}/4255\mathbb{Z}$$

$$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/169\mathbb{Z} = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/845\mathbb{Z}$$

$$\mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z} = \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/325\mathbb{Z}$$

$$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z} = \mathbb{Z}/65\mathbb{Z} \times \mathbb{Z}/65\mathbb{Z}$$

(we have the elementary divisors decomposition on the left and the invariant factors decomposition on the right).

Problem 3. a) Let $\sigma = (1, 2, 3)(4, 5) \in S_5$. List all elements of the cyclic group $< \sigma >$. For every element π of $< \sigma >$ either find an element $\tau \in S_5$ such that $\tau\sigma\tau^{-1} = \pi$ or explain why no such element exists. (4 points)

b) Prove that S_n is generated by $a = (2, 3, \dots, n)$ and $b = (1, 2)$. (4 points)

c) Let G be a group of order $2n$. The action of G on itself by left multiplication defines an injective homomorphisms $\phi : G \longrightarrow S_{2n}$. Prove that if $g \in G$ has order 2 then $\phi(g)$ is a product of n disjoint transpositions (hint: what are the fixed points of $\phi(g)$). Conclude that if n is odd then G has a normal subgroup of index 2. Hint: S_{2n} has a normal subgroup of index 2 (what is it?); can $\phi(g)$ belong to this subgroup? (4 points)

Solution: a) $\sigma = (1, 2, 3)(4, 5)$ has order 6, so the group $< \sigma >$ has 6 elements:

$$\sigma = (1, 2, 3)(4, 5),\ \sigma^2 = (1, 2, 3)^2(4, 5)^2 = (1, 3, 2),\ \sigma^3 = (1, 2, 3)^3(4, 5)^3 = (4, 5),$$

$$\sigma^4 = (1, 2, 3)^4(4, 5)^4 = (1, 2, 3),\ \sigma^5 = (1, 2, 3)^5(4, 5)^5 = (1, 3, 2)(4, 5),\ \sigma^6 = id.$$

Recall that two conjugate elements have the same order (or that two permutations are conjugate if and only if they have the same cycle structure). Thus σ can only be conjugate to σ or σ^5 (the other elements have different order and different cycle structure than σ). Clearly σ is conjugate to σ (use identity as the conjugating element). Since σ^5 has the same cycle structure as σ, they are conjugate. Recall that

$$\tau\sigma\tau^{-1} = \tau(1,2,3)\tau^{-1}\tau(4,5)\tau^{-1} = (\tau(1),\tau(2),\tau(3))(\tau(4),\tau(5)).$$

For a conjugating element we can take any any permutation τ such that $\tau(1) = 1$, $\tau(2) = 3$, $\tau(3) = 2$, $\tau(4) = 4$, $\tau(5) = 5$. Thus $\tau = (2,3)$ works:

$$(2,3)\sigma(2,3)^{-1} = \sigma^5.$$

b) Let G be the subgroup of S_n generated by a, b. Note that for $1 < i < n$ we have

$$a(1,i)a^{-1} = (a(1), a(i)) = (1, i+1).$$

Thus if $(1,i) \in G$ then $(1, i+1) \in G$. This and the fact that $b = (1,2) \in G$ imply that $(1,k) \in G$ for $k = 2, 3, \ldots, n$. Since for $i \neq k$, $i > 1, k > 1$ we have $(1,i)(1,k)(1,i) = (i,k)$, we see that G contains all transpositions and therefore $G = S_n$ (we proved in class that S_n is generated by all transpositions).

c) $\phi(g)$ is a permutation of order 2, so it is a product of disjoint transpositions. Note that g acting on G by left multiplication has no fixed points: $gh = h$ for some $h \in G$ can only happen if g is the identity. It follows that for $h \in G$ the transposition (h, gh) belongs to the cycles appearing in the permutation $\phi(g)$. Since we have $2n$ elements in G, we must have n transpositions in the cycle decomposition of $\phi(g)$. This proves that $\phi(g)$ is a product of n disjoint transpositions. In particular, if n is odd then $\phi(g)$ is an odd permutation.

For every m, the alternating group A_m is a subgroup of index 2 in S_m. If H is a subgroup of S_m then $H \cap A_m$ is a subgroup of H and $[H : H \cap A_m] \leq [S_m : A_m] = 2$. In other words, either $H \subseteq A_m$ or $[H : H \cap A_m] = 2$.

Let us apply the above observation to $H = \phi(G)$, a subgroup of S_{2n}. Since H contains an odd permutation $\phi(g)$ (assuming n is odd), H is not contained in A_{2n}. Thus $H \cap A_{2n}$ has index 2 in H. Since G is isomorphic to H, G also has a subgroup of index 2. Finally, recall that a subgroup of index 2 is always normal.

Problem 4. a) State the Nielsen-Schreier theorem. (3 points)

b) Show that the group $SL_3(\mathbb{Z})$ has a subgroup A which is free abelian of rank 2. (3 points)

c) Let H be a subgroup of $SL_3(\mathbb{Z})$ of finite index. Prove that H is not free (hint: consider $H \cap A$). (4 points)

Solution: a) **Nielsen-Schreier Theorem.** A subgroup of a free group is also a free group.

b) Consider the subgroup A of $SL_3(\mathbb{Z})$ generated by $E_{1,2}(1)$ and $E_{1,3}(1)$. Since the matrices $E_{1,2}(1)$ and $E_{1,3}(1)$ commute, the group A is abelian. Let us verify this:

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

Let $M =< E_{1,2}(1) >$ and $N =< E_{1,3}(1) >$ be the cyclic subgroups of A generated by $E_{1,2}(1)$ and $E_{1,3}(1)$ respectively. Clearly $M \cap N = \{I\}$ and $MN = A$. Thus $A = M \times N$. Since both M, N are infinite cyclic groups, A is isomorphic to $\mathbb{Z} \times \mathbb{Z}$, i.e. A is free abelian of rank 2.

Alternatively, it is straightforward to verify that the map

$$(m, n) \mapsto \begin{pmatrix} 1 & m & n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = E_{1,2}(1)^m E_{1,3}(1)^n = E_{1,2}(m) E_{1,3}(n)$$

defines a group isomorphism between $\mathbb{Z} \times \mathbb{Z}$ and A.

c) Let H be a subgroup of finite index in $SL_3(\mathbb{Z})$. Then $H \cap A$ is a subgroup of finite index in A. A subgroup of finite index in a free abelian group of rank n is also a free abelian group of rank n. Thus $H \cap A$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}$, and therefore it is not a free group. By the Nielsen-Schreier theorem, H can not be a free group.

Problem 5. Let $\mathbb{Q}$ be the group of rational numbers under addition.

a) Prove that any finitely generated subgroup of $\mathbb{Q}$ is cyclic. (3 points)

b) Let A be a finitely generated abelian group. Prove that any homomorphism $f : \mathbb{Q} \longrightarrow A$ is trivial. (hint: use the structure theorem for finitely generated abelian groups) (4 points)

c) Prove that if the elements $a_1, a_2, a_3, \ldots$ generate $\mathbb{Q}$ then the elements $a_2, a_3, \ldots$ also generate $\mathbb{Q}$. (hint: use b)) (3 points)

Solution: a) Let H be a subgroup of $\mathbb{Q}$ generated by finitely many elements $\frac{a_1}{m_1}, \frac{a_2}{m_2}, \ldots, \frac{a_k}{m_k}$. Note that each of this elements belongs to the cyclic subgroup $\left\langle \frac{1}{m_1 m_2 \ldots m_k} \right\rangle$ of $\mathbb{Q}$. Since a subgroup of a cyclic group is cyclic, H is a cyclic group.

b) Recall that a finitely generated abelian group is isomorphic to a group of the form $B\times\mathbb{Z}^n$ for some finite abelian group B and some $n\geq 0$. Let m be the order of B (if B is trivial, take any $m>1$). Suppose that $f:\mathbb{Q}\longrightarrow B\times\mathbb{Z}^m$ is a homomorphism and let $q\in\mathbb{Q}$. Then $f(q)=(b,a_1,\ldots,a_k)$ for some $b\in B$ and $a_i\in\mathbb{Z}$. For any integer $s>0$ we have $f(q/m^s)=(\hat{b},\hat{a}_1,\ldots,\hat{a}_k)$ for $\hat{b}\in B$ and $\hat{a}_i\in\mathbb{Z}$. It follows that

$$(b,a_1,\ldots,a_k)=f(q)=f(m^s{\cdot}q/m^s)=m^sf(q/m^s)=m^s(\hat{b},\hat{a}_1,\ldots,\hat{a}_k)=(m^s\hat{b},m^s\hat{a}_1,\ldots,m^s\hat{a}_k).$$

Thus $b=m^s\hat{b}=0$ (since m is the order of B) and $a_i=m^s\hat{a}_i$ for all i. This shows that a_i is divisible by m^s. Since $m>1$ and s can be chosen arbitrary, this can only happen if $a_i=0$. It follows that $f(q)=0$. Since q was arbitrary, f is the trivial homomorphism.

c) Let K be the subgroup of $\mathbb{Q}$ generated by the elements $a_2,a_3,\ldots$. Since $a_1,a_2,a_3,\ldots$ generate $\mathbb{Q}$, the group $\mathbb{Q}/K$ is cyclic generated by the image of a_1. The quotient map $\mathbb{Q}\longrightarrow\mathbb{Q}/K$ is a surjective homomorphism into a finitely generated abelian group, hence it is trivial. Since K is the kernel of this homomorphism, we get $K=\mathbb{Q}$.

****

Problem 6. Let A,B be two subgroups of finite index in a group G such that $[G:A]$ and $[G:B]$ are relatively prime. Prove that $G=AB$. Hint: Think of AB as a union of some number of cosets of B; what is this number? (5 points)

Solution: We start with a general observation. If K,H are subgroups of a group G then the subset HK is the union of all cosets hK, with $h\in H$. Two such cosets h_1K, h_2K are equal if and only if $h_1^{-1}h_2\in K$, which is the same as $h_1^{-1}h_2\in H\cap K$ (since $h_i\in H$), which is equivalent to $h_1(H\cap K)=h_2(H\cap K)$. This shows that the cosets of K appearing in HK are in bijection with the cosets of $H\cap K$ in H. In particular, HK is a union of exactlty $[H:H\cap K]$ distinct cosets of H in G.

Returning to the problem, we see that AB is the union of $[A:A\cap B]$ cosets of B. Recall now that $[G:A][A:A\cap B]=[G:A\cap B]=[G:B][B:A\cap B]$. It follows that $[G:B]$ divides $[G:A][A:A\cap B]$. Since $[G:A]$ and $[G:B]$ are relatively prime, we conclude that $[G:B]$ divides $[A:A\cap B]$. Since the number of distinct cosets of B in G is $[G:B]$ and AB is the union of $[A:A\cap B]$ of them, we conclude that $[G:B]=[A:A\cap B]$ and all cosets of B appear in AB. Thus $AB=G$ (as G is the union of all the cosests of B).

Problem 7. Let G be a finitely generated group such that $[G, G]$ is finite. Prove that $[G : Z(G)]$ is finite, where $Z(G)$ is the center of G. Hint: Show that the conjugacy class of each generator is finite; what does this tell you about the centralizer of each generator? (5 points)

Remark. The converse is also true: if $[G : Z(G)]$ is finite then $[G, G]$ is finite (but it is more difficult to prove).

Solution: Let $g_1, \ldots, g_m$ generate G. For a fixed i and $g \in G$ the element $g g_i g^{-1} g_i^{-1} \in [G, G]$, so $g g_i g^{-1} \in g_i[G, G]$. Since $g_i[G, G]$ is finite, the conjugacy class of g_i (i.e. the set of all elements conjugate to g_i) is finite. G acts transitively on the conjugacy class of g_i by conjugation and the stabilizer of g_i is the same as the centralizer of g_i. The index of the stabilizer is equal to the size of the orbit, so the centralizer $C(g_i)$ of g_i has finite index in G. It follows that the intersection $Z = C(g_1) \cap C(g_2) \cap \ldots \cap C(g_m)$ has finite index in G. Note $Z = Z(G)$ is the center of G, since an element $g \in G$ is central if and only if g commutes with each generator of G.