Peize Liu
St. Peter's College
University of Oxford

Problem Sheet 2

ASO: Group Theory

May 27, 2020

Question 1

Let A_∞ denote the even permutations of $\mathbb{N}$, thought of as

$$A_\infty = \bigcup_{n=1}^{\infty} A_n.$$

Show that A_∞ is an infinite simple group.

Proof. Suppose for contradiction that A_∞ has a non-trivial normal subgroup N. Let $\sigma \in N$ be a non-identity element. Since the elements of A_∞ are even permutations of finite subsets of $\mathbb{N}$, we may assume that σ is the permutation of a subset of $\mathbb{N}$ with n elements. It follows that $\sigma \in A_n$. Let $m = \max\{5, n\}$. We have $\sigma \in A_m$, where A_m is known to be a simple group. $\langle\sigma\rangle$ is a subgroup of N, and hence is a normal subgroup of A_∞. But we also have $\langle\sigma\rangle \leqslant A_m \leqslant A_\infty$. Then $\langle\sigma\rangle$ is normal in A_m. Since A_m is simple, either $\langle\sigma\rangle = \{e\}$ or $\langle\sigma\rangle = A_m$. It is clear that A_m is not cyclic, and $\sigma \neq e$. This leads to a contradiction. In conclusion A_∞ is simple. □

Question 2

Let G be a group and G' denote its derived subgroup. We showed in lectures that $G' \triangleleft G$.

(i) Show that if $H \triangleleft G$ and G/H is Abelian then $G' \leqslant H$.

(ii) Conversely, show that if $G' \leqslant H \leqslant G$ then $H \triangleleft G$ and G/H is Abelian.

Proof. (i) For $g, h \in H$, since G/H is Abelian, we have

$$(gH)(hH) = (hH)(gH) \implies h^{-1}g^{-1}hgH = H \implies [h,g] = h^{-1}g^{-1}hg \in H$$

Hence $G' \leqslant H$.

(ii) For $g \in G$, $h \in H$, $[g,h] \in G' \leqslant H$. Then there exists $h' \in H$ such that $ghg^{-1}h^{-1} = h' \implies ghg^{-1} = h'h \in H$. Hence $H \triangleleft G$.

Next we note that for $g, h \in G$,

$$[g,h] \in G' \implies (gG')(hG') = (hG')(gG')$$

whence G/G' is Abelian. By third isomorphism theorem, we have

$$\frac{G/G'}{H/G'} \cong G/H$$

Then G/H is a quotient of G/G' and hence is also Abelian. □

Question 3

Given two groups N, H and a homomorphism $\varphi : H \to \mathrm{Aut}(N)$, verify that the semi-direct product $N \rtimes_\varphi H$ does indeed satisfy the group axioms.

Proof. **Associativity**: For $n_1, n_2, n_3 \in N$ and $h_1, h_2, h_3 \in H$,

$$\begin{aligned}(n_1,h_1)\circ((n_2,h_2)\circ(n_3,h_3)) &= (n_1,h_1)\circ(n_2\varphi(h_2)(n_3),\ h_2h_3)\\ &= (n_1\varphi(h_1)(n_2\varphi(h_2)(n_3)),\ h_1h_2h_3)\\ &= (n_1\varphi(h_1)(n_2)\varphi(h_1h_2)(n_3),\ h_1h_2h_3)\\ &= (n_1\varphi(h_1)(n_2),\ h_1h_2)\circ(n_3,h_3)\\ &= ((n_1,h_1)\circ(n_2,h_2))\circ(n_3,h_3)\end{aligned}$$

Identity: $(e,e) \in N \rtimes_\varphi H$ is the identity. For $(n,h) \in N \rtimes_\varphi H$,

$$(n,h) \circ (e,e) = (n\varphi(h)(e),\ he) = (ne, he) = (n,h)$$
$$(e,e) \circ (n,h) = (e\varphi(e)(n),\ eh) = (e\,\mathrm{id}(n),\ h) = (n,h)$$

Inverse: For $(n,h) \in N \rtimes_\varphi H$, h induces an automorphism $\varphi_h : N \to N$. Let $n' := \varphi_h^{-1}(n^{-1}) = \varphi_{h^{-1}}(n^{-1})$. We claim that $(n,h)^{-1} = (n', h^{-1})$. Indeed,

$$(n,h) \circ (n', h^{-1}) = (n\varphi(h)(n'),\ hh^{-1}) = (nn^{-1},\ hh^{-1}) = (e,e)$$
$$(n', h^{-1}) \circ (n,h) = (n'\varphi(h^{-1})(n),\ h^{-1}h) = (\varphi(h^{-1})(n^{-1})\varphi(h^{-1})(n),\ h^{-1}h) = (\varphi(h^{-1})(e),\ h^{-1}h) = (e,e)$$

In conclusion, the semi-diract product satisfies the group axioms. □

Question 4

Verify directly Sylow's three theorems for the following groups:

$$S_3, \qquad D_{12}, \qquad A_4, \qquad S_4.$$

Proof.

1. S_3 has order $6 = 2 \times 3$. We shall count the Sylow 2-subgroups and 3-subgroups of S_3.

   S_3 has 3 2-subgroups, which are subgroups generated by transpositions:

   $$\{e, (12)\},\ \{e, (13)\},\ \{e, (23)\}$$

   Since $3 \mid 3$ and $3 \equiv 1 \pmod 2$, Sylow first and third theorem holds. It is obvious that these subgroups are conjugate with each other, so Sylow second theorem also holds.

   S_3 has a unique 3-subgroup, which is $\{e, (123), (132)\}$. Since $1 \mid 2$ and $1 \equiv 1 \pmod 3$, Sylow first and third theorem holds. It is clear that $\{e, (123), (132)\}$ is normal in S_3 because the conjugation of a 3-cycle is also a 3-cycle. Therefore Sylow second theorem also holds.

2. $D_{12} = \langle \sigma, \tau \mid \sigma^2, \tau^6, \sigma\tau\sigma\tau \rangle$ has order $12 = 4 \times 3$. We shall count the Sylow 2-subgroups and 3-subgroups of D_{12}.

   D_{12} has a unique 3-subgroup: $\{e, \tau^2, \tau^4\}$, because τ^2 and τ^4 are the only elements in D_{12} that have order 3. Since $1 \mid 4$ and $1 \equiv 1 \pmod 3$, Sylow first and third theorem holds. $\{e, \tau^2, \tau^4\}$ is a subgroup of $\langle \tau \rangle$, which is normal in D_{12}. Therefore $\{e, \tau^2, \tau^4\} \triangleleft D_{12}$ and Sylow second theorem holds.

   D_{12} has 3 2-subgroups:

   $$\{e, \sigma, \tau^3, \sigma\tau^3\},\ \{e, \sigma\tau, \tau^3, \sigma\tau^4\},\ \{e, \sigma\tau^2, \tau^3, \sigma\tau^5\}.$$

   Since $3 \mid 3$ and $3 \equiv 1 \pmod 2$, Sylow first and third theorem holds. Furthermore, these groups are conjugate with each other:

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

   Therefore Sylow second theorem holds.

3. A_4 has order $12 = 4 \times 3$. We shall count the Sylow 2-subgroups and 3-subgroups of A_4.

   We know that A_4 has an identity, 3 double transpositions, and 8 3-cycles. The identity and 3 double transpositions generates the unique 2-subgroup of A_4: $\{e, (12)(34), (13)(24), (14)(23)\}$. Since $1 \mid 3$ and $1 \equiv 1 \pmod 2$, Sylow first and third theorem holds. It is known that $\{e, (12)(34), (13)(24), (14)(23)\}$ is normal in A_4, so Sylow second theorem holds.

   The 8 3-cycles and the identity can generates 4 different 3-subgroups of A_4:

$$\{e,(123),(132)\},\ \{e,(134),(143)\},\ \{e,(124),(142)\},\ \{e,(234),(243)\}.$$

Since $4 \mid 4$ and $4 \equiv 1 \pmod 3$, Sylow first and third theorem holds. Furthermore, these groups are conjugate with each other:

$$(13)(24)\{e,(123),(132)\}(13)(24) = \{e,(134),(143)\};$$
$$(12)(34)\{e,(123),(132)\}(12)(34) = \{e,(134),(143)\};$$
$$(14)(23)\{e,(123),(132)\}(14)(23) = \{e,(234),(243)\}.$$

Therefore Sylow second theorem holds.

4. S_4 has order $24 = 8 \times 3$. We shall count the Sylow 2-subgroups and 3-subgroups of S_4.

   S_4 has 4 3-subgroups, which are the same as in A_4. Since $4 \mid 8$ and $4 \equiv 1 \pmod 3$, Sylow first and third theorem holds. Sylow second theorem holds as we have shown above.

   Now we cconsider the order 8 subgroups of S_4. By Prelim Group Theory Sheet 7 Question 5, we know that S_4 does not contain a subgroup isomorphic to C_2^3. Hence any order 8 subgroup of S_4 must contain some order 4 elements. We know that S_4 has six order 4 elements, namely the 4-cycles:

$$(1234),(1243),(1324),(1342),(1423),(1432)$$

   and we know that

$$(1234)^2 = (1432)^2 = (13)(24); \quad (1243)^2 = (1342)^2 = (14)(23); \quad (1324)^2 = (1423)^2 = (12)(34).$$

   Next, from a brilliant observation by Shuwei, any two order 4 elements in a order 8 group must have the same square. We deduce that these 6 order 4 elements belong to 3 different order 8 subgroups of S_4, each of which is isomorphic to D_8. The 2-subgroups of S_4 are:

$$\langle (1234),(13)\rangle,\ \langle (1243),(14)\rangle,\ \langle (1324),(12)\rangle.$$

   Since $3 \mid 3$ and $3 \equiv 1 \pmod 2$, Sylow first and third theorem holds. Furthermore, these groups are conjugate with each other:

$$(34)\langle (1234),(13)\rangle(34) = \langle (1243),(14)\rangle;$$
$$(23)\langle (1234),(13)\rangle(23) = \langle (1324),(12)\rangle.$$

   Therefore Sylow second theorem holds. □

Question 5

Let P be a non-trivial group of order p^m, where p is prime and $m > 0$.

By considering the conjugation action of P on itself prove that there is a non-identity element z such that $xz = zx$ for all $x \in P$.

Show that $K = \langle z \rangle$ is a normal subgroup of P.

Deduce, by induction on m, or otherwise, that finite groups of prime power order are solvable.

Proof. Let P acts on itself by conjugation. Then $xz = zx$ for each $x \in P$ implies that $\mathrm{Orb}(z)$ is a singleton. There at least one such singleton orbit, namely $\{e\}$. By Orbit-Stabilizer Theorem, all the orbits has size p^k for some $0 \leqslant k \leqslant m$. Since the orbits of P partitions P, we have

$$N_0 + N_1 p + N_2 p^2 + \cdots + N^{m-1} p^{m-1} = p^m$$

where N_i the number of orbits of size p^i. We deduce that $p \mid N_0$. So there exists at least $p-1$ non-trivial elements in the center of P.

It is trivial that if $zx = xz$ for all $x \in P$, then $\langle z \rangle$ is normal in P.

We shall use induction on m to show that if $|P| = p^m$ then P is solvable.

If $m = 1$, then $P \cong C_p$ is trivially solvable.

Suppose that for $n < m$, the groups of order p^n are solvable.

We have proven $Z(P) \neq \{e\}$. We pick $z \in Z(P)\backslash\{e\}$. If $\langle z \rangle = P$, then P is cyclic and hence is solvable. If $\langle z \rangle \neq P$, then we have

$$p^m = |P| = |\langle z \rangle| \cdot |P/\langle z \rangle|.$$

Therefore $|\langle z \rangle| = p^r$ and $|P/\langle z \rangle| = p^s$ for some $r, s < m$. By induction hypothesis $\langle z \rangle$ and $P/\langle z \rangle$ are both solvable. Then by Theorem 59 in the notes we know that P is solvable. □

Question 6

Show that a group of order 1694 is solvable.

Proof. Note that $1694 = 2 \times 7 \times 11^2$. Let G be this group. Suppose that G has n Sylow 11-subgroups. Then by Sylow third theorem, we have $n \equiv 1 \pmod{11}$ and $n \mid 14$. Hence $n = 1$ and G has a unique Sylow 11-subgroup. Let H be this subgroup. By Sylow second theorem, $H \lhd G$. H is solvable by Question 5 above. In addition, $|G/H| = 14$. Since the only groups of order 14 are the cyclic group C_{14} or the dihedral group D_{14}, both of which are solvable, we know G/H is solvable. By Theorem 59 in the notes, G is solvable. □

Question 7

Let G be a group of order 30.

(i) Explain why one of the following holds:

- There is a normal subgroup N of order 5 and a subgroup H of order 3;
- There is a normal subgroup N of order 3 and a subgroup H of order 5;

Deduce that G has a cyclic normal subgroup K of order 15.

(ii) Let y be a generator of K and x be an order 2 element. Show that

$$G = \{x^i y^j : 0 \leqslant i \leqslant 1, \ 0 \leqslant j \leqslant 14\}$$

and that $G \cong C_{15} \rtimes_\varphi C_2$ where $\varphi : C_2 \to \mathrm{Aut}(C_{15})$ is a homomorphism.

(iii) Let ψ be an automorphism of K such that $\psi(\psi(y)) = y$. Show that $\psi(y) = y$ or y^4 or y^{11} or y^{14}.

(iv) Deduce that there are (up to isomorphism) at most four groups of order 30. Show that there are precisely four by exhibiting four non-isomorphic groups of order 30.

Proof. (i) Since G has order $30 = 2 \times 3 \times 5$, by Sylow first theorem, G has Sylow 3-subgroups and 5-subgroups. Suppose that G has n 3-subgroups and m 5-subgroups. By Sylow third theorem, we have $n \equiv 1 \pmod 3$ and $n \mid 10$. Then $n = 1$ or 10. $m \equiv 1 \pmod 5$ and $m \mid 6$. Then $m = 1$ or 6.

Suppose for contradiction that G has no normal subgroups of order 3 and 5. Then G has 10 Sylow 3-subgroups and 6 Sylow 5-subgroups. It follows that G has at least $10(3-1) = 20$ order 3 elements and $6(5-1) = 24$ order 5 elements. But G has only 30 elements, which is a contradiction. Hence G has either a normal subgroup of order 3 or of order 5 (or both).

By third isomorphism theorem $K := HN \leqslant G$. Since $|HN| = |H||N|/|H \cap N| = 15$, HN is a index 2 subgroup in G, so it is normal. By Proposition 95 in the notes, any group of order 15 is cyclic. So HN is cyclic.

(ii) It suffices to show that $x^i y^j$ are distinct for $0 \leqslant i \leqslant 1,\ 0 \leqslant j \leqslant 14$. For $x^{i_1}y^{j_1} = x^{i_2}y^{j_2}$, we have $x^{i_1-i_2}y^{j_1-j_2} = e$. If $i_1 \neq i_2$, then $y^{j_1-j_2} = x$, which is contradictory since $K \cap \langle x \rangle = \{e\}$. Then $i_1 = i_2$ so that $y^{j_1-j_2} = e$. Since y generates $K \cong C_{15}$, $(j_1 - j_2) \mid 15$. It follows that $j_1 = j_2$. So the claim is proven. Since $|G| = 30$ and $|\{x^i y^j : 0 \leqslant i \leqslant 1,\ 0 \leqslant j \leqslant 14\}| = 30$, the result follows.

Since $K \lhd G$, $\langle x \rangle \lhd G$, and $K \cap \langle x \rangle = \{e\}$, by defintion $G = K \rtimes \langle x \rangle$. The internal semi-direct product induces $\varphi : \langle x \rangle \to \mathrm{Aut}(K)$ by $\varphi_x : g \mapsto xgx$ and $\varphi_e = \mathrm{id}$. This gives the isomorphism with the external semi-direct product: $G = C_{15} \rtimes_\varphi C_2$.

(iii) Suppose that $\psi(y) = y^n$. Then $\psi(\psi(y)) = y^{n^2}$. $\psi \circ \psi(y) = y \implies n^2 \equiv 1 \pmod{15}$. Then $15 \mid (n+1)(n-1)$. There are 4 possibilities:

$$\begin{cases} n \equiv -1 \pmod 3 \\ n \equiv 1 \pmod 5 \end{cases} \qquad \begin{cases} n \equiv 1 \pmod 3 \\ n \equiv -1 \pmod 5 \end{cases} \qquad n \equiv -1 \pmod{15} \qquad n \equiv 1 \pmod{15}$$

By Chinese Remainder Theorem the solutions of these equations are unique in C_{15}. The solutions are $n = 11$, $n = 4$, $n = 14$ and $n = 1$. Hence $\psi(y) = y$ or y^4 or y^{11} or y^{14}.

(iv) Since $C_{15} \rtimes_\varphi C_2$, and $\varphi : C_2 \to \mathrm{Aut}(C_{15})$ is a group homomorphism,

$$y = \mathrm{id}(y) = \varphi(e)(y) = \varphi(x^2)(y) = \varphi(x) \circ \varphi(x)(y)$$

Then by part (iii), $\varphi(x)(y) = y$ or y^4 or y^{11} or y^{14}. There are at most 4 different homomorphisms φ, so there are at most 4 non-isomorphic groups of order 30. The four non-isomorphic groups of order 30 are:

$$C_{30}, \qquad D_{30}, \qquad D_{10} \times C_3, \qquad S_3 \times C_5.$$

□