**Interview Questions on Algebra**

*Wenhan Dai*

## Set II: Classification of Finite Groups

1. Given a finite abelian group with at most $n$ elements of order divisible by $n$, prove it's cyclic.

   *Comment.* It seems that some ambiguity lies in the question. But arguments like this essentially relies on Cauchy's theorem, Cayley's theorem, and Sylow's theorems to compute orders.

2. Suppose I asked you to classify groups of order 4. Why isn't there anything else? Which of those could be realised as a Galois group over $\mathbb{Q}$?

   *Answer.* Since groups of order $p^2$ are all abelian, there are two types up to isomorphism: $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

3. State/prove the Sylow theorems.

   *Statement.* The Sylow theorems are in the following:

   (I) $p$-Sylow subgroup exists in a finite group and contains all $p$-subgroups.

   (II) All $p$-Sylow subgroups are mutually conjugate.

   (III) The number of $p$-Sylow subgroups satisfies

   $$n_p \equiv 1 \bmod p, \quad n_p \mid m,$$

   where $|G| = p^k m$ and $p \nmid m$.

   (III*) Let $N(P)$ be the normalizer of a Sylow $p$-subgroup $P$. Then $n_p = [G : N(P)]$.

   *Proof.* Using group actions and the fact: when a finite $p$-group $\Gamma$ acts on a finite set $X$, we would say

   $$|X| \equiv |\operatorname{Fix}_\Gamma(X)| \bmod p.$$

   The strategy of group actions at work:

| Theorem | Group | Set | Action |
|---|---|---|---|
| Sylow I | $p$-subgroup $H$ | $G/H$ | left multiplication |
| Sylow II | $Q \in \mathrm{Syl}_p(G)$, $Q \neq P$ | $G/P$ | left multiplication |
| Sylow III: $n_p \equiv 1 \bmod p$ | $P \in \mathrm{Syl}_p(G)$ | $\mathrm{Syl}_p(G)$ | conjugation |
| Sylow III: $n_p \mid m$ | $G$ | $\mathrm{Syl}_p(G)$ | conjugation |
| Sylow III* | $G$ | $\mathrm{Syl}_p(G)$ | conjugation |

   (I) Consider the series

   $$\{e\} = H_0 \subset H_1 \subset \cdots, \quad |H_i| = p^i, \quad 0 \le i \le k.$$

   Choose some $H = H_j$ in this series that acts on the coset $G/H$ (need not be a group), then

   $$|G/H| \equiv |\operatorname{Fix}_H(G/H)| \bmod p.$$

Also note that

$$\mathrm{Fix}_H(G/H) = \{gH : g \in N(H)\} = N(H)/H,$$

where $N(H) = \{g \in G : g^{-1}Hg = H\}$. If $p \mid |G/H|$, then a subgroup of order $p$ lies in $N(H)/H$. Switch to consider $H = H_{j+1}$ and iterate this process until $p \nmid |G/H|$ and $N(H) = H$.

(II) To show two $p$-Sylow subgroups $P, Q$ are conjugate: if $Q$ acts on $G/P$ by left multiplication, then

$$m = |G/P| \equiv |\mathrm{Fix}_Q(G/P)| \neq 0 \bmod p.$$

So there is some $gP \in G/P$ that is fixed by $Q$. Hence $QgP = gP$ and $Q = gPg^{-1}$ since they have the same size.

(III) Let $P$ act on $\mathrm{Syl}_p(G)$ by conjugation:

$$n_p = |\mathrm{Syl}_p(G)| \equiv |\mathrm{Fix}_P(\mathrm{Syl}_p(G))| \bmod p.$$

The fixed points are $\{Q \in \mathrm{Syl}_p(G) : pQp^{-1} = Q, \forall p \in P\}$. For any $Q$, Sylow II shows that $P, Q$ are conjugate normal subgroups of $N(Q)$. But there's only one conjugate class, so $P = Q$ and $n_p \equiv 1 \bmod p$.

By orbit-stabilizer formula, if $G$ acts on $X$ with one orbit, then $|X|$ divides $|G|$. Now, let $G$ act on $\mathrm{Syl}_p(G)$ by conjugation. By Sylow II, the orbit is unique. Thus, $n_p \mid |G|$ but $n_p \equiv 1 \bmod p$, and therefore $n_p \mid m$.

(III*) By the orbit-stabilizer formula,

$$n_p = |\mathrm{Syl}_p(G)| = [G : \mathrm{Stab}_P].$$

The stabilizer views $P$ as a point of $\mathrm{Syl}_p(G)$ and

$$\mathrm{Stab}_P = \{g : gPg^{-1} = P\} = N(P).$$

Thus $n_p = [G : N(P)]$ and we're done.

4. Classify groups of order 35.

*Solution.* By Sylow, any group of order $pq$ with $p < q$ and $p \nmid (q-1)$ should be cyclic, because $n_p = n_q = 1$. So $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} = \mathbb{Z}/35\mathbb{Z}$ is the only group of order 35.

5. Classify groups of order 21.

*Recipe.* A group of order $pq$ with $p < q$ and $q \equiv 1 \bmod p$ has two types: $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ and $\mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$, where

$$\begin{aligned} \varphi : \mathbb{Z}/p\mathbb{Z} &\longrightarrow \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \\ b \bmod p &\longmapsto \mathrm{mult}_{x^b}. \end{aligned}$$

The operation in semidirect product is given by

$$(a, b)(c, d) = (a + x^b c, b + d)$$

for some $x \in \mathbb{Z}/q\mathbb{Z}$ satisfying $x \neq 1$ and $x^p \equiv 1 \bmod q$.

*Solution.* For nonabelian $G$ with $|G| = 21$, we see $G \cong \mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$ whose operation is $(a, b)(c, d) = (a + 2^b c, b + d)$.

6. Discuss groups of order 55.

   *Solution.* Same argument as in Question 5.

7. Classify groups of order 14. Why is there a group of order 7? Are all index-2 subgroups normal?

   *Answer.* Up to isomorphisms, any group of order 14 is either cyclic or $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. There is a normal subgroup $N_7$ by Sylow, because of $n_7 = 1$. Are all index-2 subgroups are normal (see Question 2 of Set I).

8. How many groups are there of order 15? Prove it.

   *Solution.* Only one, say $\mathbb{Z}/15\mathbb{Z}$. See Question 4 where Sylow's theorems were used.

9. Classify all groups of order 8.

   *Solution.* There are three types of abelian groups of order 8. As for the nonabelian case, note that all elements are of order 2 or 4 (but all $g \in G$ cannot have the same order, otherwise $G$ is abelian). Then

$$G = \langle x, y \rangle, \quad x^4 = y^4 = 1, \quad x^3 \neq 1.$$

   The index-2-subgroup $\langle x \rangle$ is normal in $G$. So $yxy^{-1}$ is a power of $x$ whose order is 4, namely $yxy^{-1} = x^3 = x^{-1}$ since $G$ is nonabelian. On the other hand, $y^2 \in \langle x \rangle$ has order 1 or 2 such that

$$\begin{aligned} \text{either} \quad & x^4 = 1, \quad y^2 = 1, \quad yxy^{-1} = x^{-1} \quad \Longrightarrow \quad G = D_4; \\ \text{or} \quad & x^4 = 1, \quad y^2 = x, \quad yxy^{-1} = x^{-1} \quad \Longrightarrow \quad G = Q_8. \end{aligned}$$

   Here the quaternion group

$$Q_8 = \langle i, j : i^2 = j^2 = -1, iji^{-1} = j^{-1} \rangle \cong \mathbb{Z}/4\mathbb{Z} \rtimes_\varphi \mathbb{Z}/4\mathbb{Z}/\langle (2,2) \rangle,$$

   in which $\varphi$ induces $(a, b)(c, d) = (a + (-1)^b c, b + d)$. So there are in total 2 nonisomorphic nonabelian groups of order 8.

10. Classify all groups of order $p^3$ for $p$ prime.

    *Result.* See the proceeding Question 9 for $p = 2$. When $p \neq 2$, nonabelian groups of order $p^3$ has two types. The Heisenberg group

$$\mathrm{Heis}(\mathbb{Z}/p\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}/p\mathbb{Z} \right\},$$

    and a nameless one

$$G_p = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in \mathbb{Z}/p^2\mathbb{Z}, a \equiv 1 \bmod p \right\}.$$

11. What are the groups of order $p^2$? What about $pq$? What if $q \equiv 1 \bmod p$?

    *Answer.* Any group of order $p^2$ should be abelian, so there are only two groups of order $p^2$ for a fixed $p$. This is because all $p$-groups have nontrivial centers (see Question 13

in Set I), either $|G/Z(G)| = p$ or $|G/Z(G)| = 1$, and $G/Z(G)$ must be cyclic. Thus, $G$ is abelian.

By Sylow, any group of order $pq$ with $p < q$ and $p \nmid (q-1)$ should be cyclic, because $n_p = n_q = 1$. No matter what $p, q$ are, we always obtain $n_q = 1$. When $q \equiv 1 \bmod p$, note that $N_q \cong \mathbb{Z}/q\mathbb{Z}$ is a normal subgroup. Then the only possibility is that this group is isomorphic to the semi-direct product $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$.

12. What are the groups of order 12? Can there be a group of order 12 with 2 nonisomorphic subgroups of the same order?

*Solution.* The abelian ones are $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$. The nonabelian ones are $A_4, D_6$, and $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$ (where the semidirect product is unique). These are all given by 4 distinct semidirect products.

*Answer.* There cannot exist two nonisomorphic subgroups. Suppose not, then the order is not a prime, and must be 4 or 6. Since the subgroup of index 2 is normal and the two normals are in the same conjugate orbit (so they are isomorphic), this order cannot be 6. Again, since all groups of order $p^2$ are abelian, there are only 2 types in consideration: $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Any group of order 12 cannot contain both of them.

*Remark.* For another example, the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ of order 8 contains both of them simultaneously.

13. How would you start finding the groups of order 56? Is there in fact a way for $\mathbb{Z}/7\mathbb{Z}$ to act on a group of order 8 nontrivially?

*Fact.* Any group of order $p(p+1)$ that contains no normal Sylow subgroup is in the form $\mathbb{F}_{2^N} \rtimes \mathbb{F}_{2^N}^\times$ for $p = 2^N - 1$. This is proved by claiming that elements whose orders do not divide $p$ forms a conjugate class.

*Answer.* Consider $H \rtimes \mathbb{Z}/7\mathbb{Z}$ where $H$ is normal of order 8. For the classification of $H$, see Question 9.

- $H = \mathbb{Z}/8\mathbb{Z}$: here $\mathbb{Z}/7\mathbb{Z} \to \mathrm{Aut}(H) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ should be trivial.
- $H = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$: here $7 \nmid \mathrm{Aut}(H)$, and there is no nontrivial action.
- $H = (\mathbb{Z}/2\mathbb{Z})^3$: here $\mathrm{Aut}(H) = \mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$ whose order is $(2^3-1)(2^3-2)(2^3-2^2) = 7 \cdot 24$, hence there is a nontrivial action.
- $H = D_4$: the fact at work is

$$\mathrm{Aut}(D_n) \cong \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in (\mathbb{Z}/n\mathbb{Z})^\times, b \in \mathbb{Z}/n\mathbb{Z} \right\} \cong \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times.$$

In particular, it has order $n\varphi(n)$. This is loosely because any $f \in \mathrm{Aut}(D_n)$ maps any element outside $\langle r \rangle$ to an order 2 element, hence $f(\langle r \rangle) = \langle r \rangle$. Then

$$f(r) = r^a, \quad f(s) = r^b s.$$

The uniqueness and the group law can be furthermore checked directly.

Thus $\mathrm{Aut}(D_4) \cong D_4$ that admits no nontrivial $\mathbb{Z}/7\mathbb{Z}$-action.

- $H = Q_8$: the fact at work is $\mathrm{Aut}(Q_8) \cong S_4$, and for $n \geq 4$

$$\begin{aligned}\mathrm{Aut}(Q_{2^n}) &\cong \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in (\mathbb{Z}/2^{n-1}\mathbb{Z})^\times, b \in \mathbb{Z}/2^{n-1}\mathbb{Z} \right\} \\ &\cong \mathbb{Z}/2^{n-1}\mathbb{Z} \rtimes (\mathbb{Z}/2^{n-1}\mathbb{Z})^\times.\end{aligned}$$

  The reason is similar to the case of dihedral groups.

  Thus $\mathrm{Aut}(Q_8) \cong S_4$ that admits no nontrivial $\mathbb{Z}/7\mathbb{Z}$-action.

14. How many abelian groups are there of order 36?

    *Solution.* The answer is 4. These abelian groups are

$$\begin{aligned}&\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \\ &\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \\ &\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}, \\ &\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}.\end{aligned}$$

15. What are the abelian groups of order 16?

    *Solution.* They are given by

$$\begin{aligned}&(\mathbb{Z}/2\mathbb{Z})^4, \quad (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/4\mathbb{Z}, \\ &(\mathbb{Z}/4\mathbb{Z})^2, \quad \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/16\mathbb{Z}.\end{aligned}$$

    *Remark.* In general, for the abelian group of order $p^n$, the number of non-isomorphic types is equal to the number of partitions of $n$.

16. What are the abelian groups of order 9? Prove that they are not isomorphic. Groups of order 27?

    *Answer.* All group of order 9 are abelian, and they are $\mathbb{Z}/9\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. They are not isomorphic because the latter one doesn't has any element of order 9, whereas the former one does.

    Similarly, there are three types of abelian groups of order 27, say $\mathbb{Z}/27\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, and $(\mathbb{Z}/3\mathbb{Z})^3$. They are mutually non-isomorphic.

17. How many abelian groups of order 200 are there?

    *Solution.* Since $200 = 2^3 \cdot 5^2$, and $2^3, 5^2$ respectively has 3 and 2 division types (namely, different partitions), there are 6 abelian groups of order 200.

18. Prove there is no simple group of order 132.

    *Proof.* Suppose $G$ is a simple group with order $|G| = 132 = 2^2 \cdot 3 \cdot 11$. Then $n_{11} \equiv 1 \bmod 11$ and $n_{11} \mid 12$, which implies $n_{11} = 12$ by assumption (otherwise $n_{11} = 1$ and $N_{11}$ is a normal subgroup). By Sylow again together with $n_3 \neq 1$, it turns out to be $n_3 \geq 4$. Then there are $(11-1)n_{11} = 120$ elements of order 11 and at least $(3-1)n_3 = 8$ elements of order 3. This forces the number of elements of order 2 to be 3, and hence $n_2 = 1$. This means $N_2$ is a normal subgroup, which leads to a contradiction.

19. Prove that there is no simple group of order 160. What can you say about the structure of groups of that order?

    *Proof.* Note that $160 = 2^5 \cdot 5$ and $n_2 = 1$ or 5 by Sylow. In the later case $G$ acts on 5 distinct Sylow subgroups by conjugation transitively by Sylow. Therefore, we get a non-trivial homomorphism $G \to S_5$ whose order is 120. Therefore the kernel has order greater than 1 and is a non-trivial normal subgroup.

    *Answer.* All groups of order $p^a q^b$ are solvable. In this case, it is $\mathbb{Z}/5\mathbb{Z} \rtimes H$, where $H$ can be realized as a subgroup of order 32.

20. Prove that there is no simple group of order 40.

    *Proof.* For $|G| = 40 = 2^3 \cdot 5$, we obtain $n_5 \equiv 1 \bmod 5$ and $n_5 \mid 8$ by Sylow. Thus $n_5 = 1$ and therefore the Sylow 5-group, say $N_5$, is a normal subgroup.