Interview Questions on Algebra

Wenhan Dai

Set I: Groups

1. What is a normal subgroup? Can you get some natural map from a normal subgroup? What topological objects can the original group, normal subgroup, and quotient group relate to?

   Answer. A subgroup $H \subseteq G$ is normal if all conjugation of H is itself, i.e. $\forall g \in G$, $H = g^{-1}Hg$. The normal subgroup defines the quotient group. The natural map is $H \hookrightarrow G \to G/H$. "Sub" means embedding, and "quotient" means gluing.

2. Prove that a subgroup of index two is normal.

   Proof. There is no position for distinct gH and Hg.

3. Find all normal subgroups of A_4.

   Solution. Note that $\#A_4 = 12$. By Sylow's Theorem, $n_2 = 1$ and either $n_3 = 1$ or $n_3 = 4$. Only the latter is possible because we obtain 3 elements of order 2 or 4, and 8 elements of order 3.

   - Order 4: $\{1, (12)(34), (13)(24), (14)(23)\} = K$, Klein 4-group.
   - Order 3: $\{1, (234), (243)\}$, $\{1, (134), (143)\}$, $\{1, (124), (142)\}$, $\{1, (123), (132)\}$.
   - Order 2: $\{1, (12)\}$, $\{1, (13)\}$, ...

4. Give an example of a non-normal subgroup. Is $\mathrm{SO}_2(\mathbb{R})$ normal inside $\mathrm{SL}_2(\mathbb{R})$?

   Example. In S_3, $n_2 = 3$ and the order 2 subgroup $\{1, (12)\}$ is not normal.

   Answer. $\mathrm{SO}_2(\mathbb{R})$ is normal. Apply **Iwasawa decomposition** to $\mathrm{SL}_2(\mathbb{R}) = KAN$:

   $$\forall g \in \mathrm{SL}_2(\mathbb{R}), \quad g = kan = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} r & 0 \\ 0 & 1/r \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \quad r > 0.$$

   It means that the geometric action of $\mathrm{SL}_2(\mathbb{R})$, on $\mathbb{H}$, for example, can be decomposed into a shearing, a stretching that preserves areas, and a rotation.

   Fact. For sufficiently nice continuous group action $G \times X \to X$ on a locally compact and Hausdorff topological space, choosing $x \in X$, the orbit map

   $$G/\operatorname{Stab}_G(x) \longrightarrow G.x$$

   is a homeomorphism.

   Alternative Answer. Using the proceeding fact: note that $\mathrm{SL}_2(\mathbb{R})$ has a transitive action towards $x = i \in \mathbb{H} = X$, and $\operatorname{Stab}_{\mathrm{SL}_2(\mathbb{R})}(i) = \mathrm{SO}_2(\mathbb{R})$. This construction naturally gives $\mathrm{SL}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R}) \cong \mathbb{H}$. The normality is automatically implied.

5. Is normality transitive? That is, is a normal subgroup of a normal subgroup normal in the biggest group?

   Answer. No. Say $K \triangleleft H$ and $H \triangleleft G$. Then $G - H$ preserves H but not necessarily preserves K.

Counterexample. A typical situation is when H is abelian, e.g.

$$G = (\mathbb{Z}/p\mathbb{Z})^2 \rtimes S_2, \quad H = (\mathbb{Z}/p\mathbb{Z})^2;$$

here the semi-direct product is by letting S_2 to permute the two factors. If we take K to be the first factor $\mathbb{Z}/p\mathbb{Z}$ of H, then K is clearly normal in H yet not normal in G.

6. Define solvable group. Give an example of a solvable nonabelian group. Show S_4 is solvable. Do the Sylow theorems tell you anything about whether the index 3 subgroup of A_4 is normal?

   Answer. G is solvable if it has a subnormal series $G = G_0 \geq G_1 \geq \cdots \geq G_n = 1$, where each G_i/G_{i+1} is abelian. S_4 is nonabelian but solvable, because $S_4 \rhd A_4 \rhd K \rhd 1$, with quotients

   $$S_4/A_4 \cong \mathbb{Z}/2\mathbb{Z}, \quad A_4/K \cong \mathbb{Z}/3\mathbb{Z}, \quad K \cong \mathbb{Z}/2 \times \mathbb{Z}/2.$$

   By Sylow, $n_2 = 1$ so K is normal.

7. Define lower central series, upper central series, nilpotent and solvable groups.

   Answer. Lower central series is $G = G_0 \geq G_1 \cdots \geq G_n \geq \cdots$, where $G_{i+1} = [G, G_i] = [G_i, G]$. Upper central series is $1 = Z_0 \leq Z_1 \leq Z_2 \leq \ldots \leq Z_n \leq \ldots$, such that $Z_1 = C(G)$, and for $n > 1$, Z_n is the unique subgroup of G such that $Z_n/Z_{n-1} = C(G/Z_{n-1})$.

   If the upper central series terminate with G, then G is called nilpotent. If the lower central series terminate with 1, then G is called solvable.

8. Define the commutator. Define the derived series. State and prove two nontrivial theorems about derived series.

   Answer. For elements $g, h \in G$ the commutator is $[g, h] = g^{-1}h^{-1}gh$. The derived series of a group is a sequence of subgroups defined recursively: the first term of the series is just the group itself, and each successive term is defined as the commutator subgroup of the previous term, i.e. $G^{(0)} = G$ and $G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$ for $n \in \mathbb{N}$.

   Results. We have two significant results about solvability:

   - Say G is solvable if and only if it has a finite derived series that terminates in the trivial subgroup, i.e. $G^{(n)} = G^{(n+1)} = \{1\}$ for some $n \gg 0$.
   - If N is a normal subgroup of G and both N and G/N are solvable, then so also is G. If H is any subgroup of G then $H^{(i)} \leq G^{(i)}$.

9. Prove that $\mathrm{SL}_2(\mathbb{Z})$ is not solvable.

   Proof. It contains the Sanov subgroup

   $$S = \left\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\rangle,$$

   which is free of rank 2, hence is not solvable (given by **Ping-Pong Lemma**).

   Lemma. If G acts on a set X, and $a, b \in G$ and $A, B \subseteq X$ are such that neither A nor B is contained in the other. Suppose that $b^n(A) \subseteq B$ and $a^n(B) \subseteq A$ for all $n \neq 0$. Then $\langle a, b \rangle$ is a free subgroup of G. Here we take $G = \mathrm{SL}_2(\mathbb{Z})$, $X = \mathbb{Z}^2$, $A = \{(x, y) : |y| > |x|\}$, $B = \{(x, y) : |x| > |y|\}$.

10. What are all possible orders of elements of $\mathrm{SL}_2(\mathbb{Z})$?

    Solution. The fact is that $\mathrm{SL}_2(\mathbb{Z}) = \langle S, T\rangle$, where

    $$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

    Here $S^2 = -I$ and S has order 4, while T has infinite order but ST has order 6. So all possible orders are factors of 12. In fact, every group homomorphism $\mathrm{SL}_2(\mathbb{Z}) \to \mathbb{C}^\times$ has image in μ_{12}.

11. Can you show that all groups of order p^n for p prime are solvable? Do you know how to do this for groups of order $p^r q^s$?

    Proof. For $n = 1$, G is cyclic and abelian. And all abelian groups are solvable. Assume groups of order p^k are solvable for all $k < n$. Let G be of order p^n. By Question 13 below, $|Z(G)| > 1$, so $|Z(G)| = p^{n-m}$ with $|G/Z(G)| = p^m$ for $m < n$, and hence both $Z(G)$ and $G/Z(G)$ are solvable. Since $Z(G)$ is normal in G, by the second theorem in Question 8, we see G is solvable.

    Comment. The second statement is Burnside's theorem, which has a classical proof using representation theory. The sketch is as follows:

    - G is simple with $Z(G) = \{1\}$.
    - There is some $g \in G$ with exactly q^d conjugates for $d > 0$.
    - There exists a nontrivial irreducible representation ρ with character χ, such that $q \nmid \dim \rho$ and $\chi(g) \in \mathbb{C}\backslash\{0\}$.
    - $\rho(g)$ is homothety, and hence $\rho(g)$ is central in $\rho(G)$, but $g \notin Z(G)$.

    Recently, there arises a purely group-theoretic but more complicated proof.

12. Suppose a p-group G acts on a set S whose cardinality is not divisible by p. Prove that there is a fixed point for the action.

    Proof. Suppose not, and then each orbit of S under the action of G has at least two elements. By orbit-stabilizer formula, the size of orbits must divide $|G|$, hence is divided by p. Note that all these orbits are disjoint such that $|X|$ is a sum of powers of p, which leads to a contradiction.

13. Prove that the centre of a group of order p^r is not trivial.

    Proposition. (Center-counting formula) Define $Z(g) := \{s \in G : sg = gs\}$ as the centralizer of $g \in G$. Let $C_1, \ldots, C_n$ be conjugacy classes of G whose representatives are $g_1, \ldots, g_n$. Note that $|C_i| = [G : Z(g_i)]$, and $g_i \in Z(G) = \{g \in G : sg = gs, \forall s \in G\}$ if and only if $|C_i| = 1$. Therefore,

    $$|G| = \sum_{i=1}^{r} [G : Z(g_i)] = \sum_{i=1}^{r} \frac{|G|}{|Z(g_i)|} = |Z(G)| + \sum_{j \in J} \frac{|G|}{|Z(g_j)|},$$

    where the index set $J = \{1 \leq j \leq n : |C_j| > 1\}$.

    Proof. Suppose $|G| = p^r$, and note that $[G : Z(g_j)] \mid p^r$ deduces $p \mid [G : Z(g_j)]$ for $j \in J$. This shows that $|Z(G)| > 1$.

14. Give examples of simple groups. Are there infinitely many?

    Answer. It turns out that A_n for all $n \geq 5$ are simple. Hence there are infinitely many simple groups. See Question 21 for proof.

15. State and prove the Jordan–Hölder theorem for finite groups.

    Statement. The composition series of G is unique up to "quotient permutations". That is, if

    $$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_r = G, \quad \{e\} = \widetilde{G}_0 \lhd \widetilde{G}_1 \lhd \cdots \lhd \widetilde{G}_s = G$$

    are both composition series for G (that means the factors, i.e. quotients of successive two subgroups, in both series are simple groups) then $r = s$ and there is $\pi \in S_r$ such that $\widetilde{G}_i/\widetilde{G}_{i-1} \cong G_{\pi(i)}/G_{\pi(i)-1}$ for $1 \leq i \leq r$.

    Proof. The ingredient is **Schreiers refinement theorem**. If a group admits two composition series then Schreiers says they can be refined to two normal series whose factor groups coincide up to isomorphism, counting multiplicity. The key feature of a composition series is that it can only be refined in a trivial way.

16. What's Cayley's theorem? Give an example of a group of order n that embeds in S_m for some m smaller than n. Give an example of a group where you have to use S_n.

    Answer. If G admits an action on some set X by left-multiplication, say $G \times X \to X$, then each $g \in G$ defines a permutation on X. Hence there is a natural map

    $$G \longrightarrow \mathrm{Sym}(X) \cong S_{|X|}.$$

    In particular, any finite group G embeds into some permutation group $S_{|G|}$.

    Example. Let G be a group of order n and $H \leq G$ be a subgroup of index m. Taking $X = G/H$ as the coset, we see

    $$G \longrightarrow \mathrm{Sym}(G/H) \cong S_m.$$

    Here G embeds into S_m for $m \leq n$. When $H = \{1\}$, we have to use S_n instead of S_m.

17. Is A_4 a simple group? What are the conjugacy classes in S_4? What about in A_4?

    Answer. A_4 is not simple because $V \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is a normal subgroup in it. The 5 conjugacy classes in S_4 are represented by

Representatives in S_4	(1)	(12)(34)	(12)	(1234)	(123)
Size of Classes in S_4	1	3	6	6	8

Also, there are 4 conjugacy classes in A_4:

Representatives in A_4	(1)	(12)(34)	(123)	(132)
Size of Classes in A_4	1	3	4	4

Note that (123) and (132) are conjugate in S_4 whereas not in A_4.

18. Talk about conjugacy classes in the symmetric group S_n.

    Fact. For each cycle $(i_1\ i_2\ \cdots\ i_k)$ in S_n and each $\sigma \in S_n$,

    $$\sigma(i_1\ i_2\ \cdots\ i_k)\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_k)).$$

    Proposition. All cycles of the same length in S_n are conjugate. Any two permutations are conjugate in S_n if and only if they share the same cycle type. For example,

    $$\pi_1 = (\underbrace{a_1\ a_2\ \cdots\ a_{m_1}}_{m_1 \text{ terms}})(\underbrace{a_{m_1+1}\ a_{m_1+2}\ \cdots\ a_{m_1+m_2}}_{m_2 \text{ terms}})\cdots,$$
    $$\pi_2 = (\underbrace{b_1\ b_2\ \cdots\ b_{m_1}}_{m_1 \text{ terms}})(\underbrace{b_{m_1+1}\ b_{m_1+2}\ \cdots\ b_{m_1+m_2}}_{m_2 \text{ terms}})\cdots$$

    has the same type $(m_1, m_2, \ldots)$ so they are conjugate.

19. When do conjugacy classes in S_n split in A_n?

    Answer. A conjugacy class in S_n split in A_n if and only if its cycle type consists of distinct odd integers. Otherwise, it remains a single conjugacy class in A_n. For example, in S_3, $(23)(123)(23) = (132)$, but (123) and (132) are not conjugate in A_3 because of $(23) \notin A_3$.

20. What is the center of S_n? Prove it.

    Answer. Let's claim $Z(S_n) = \{1\}$. Suppose not and any nontrivial element σ in it must commute with all transpositions. Since σ has order at least 2, a non-disjoint transposition gives the contradiction.

21. Prove that the alternating group A_n is simple for $n \geq 5$.

    Answer. The proof is tedious and heavy. Refer to any group-theoretical reference. For example, see Theorem 1.1 of Keith Conrad's expository paper (available at `https://kconrad.math.uconn.edu/blurbs/grouptheory/Ansimple.pdf`).

22. Prove the alternating group on n letters is generated by the 3-cycles for $n \geq 3$.

    Proof. Note that the product of two transpositions (whether or not they are disjoint) is always a product of 3-cycles:

    $$(a_1\ a_2)(b_1\ b_2) = (a_1\ b_1\ a_2)(b_1\ b_2\ a_1).$$

    On the other hand, any $\sigma \in A_n$ can be written as a product of an even number of transpositions. Hence σ is the product of 3-cycles. The converse direction is obvious.

23. Prove that for p prime, S_p is generated by a p-cycle and a transposition.

    Proof. The key ingredient is the following fact.

    ◇ For $1 \leq a < b \leq n$, the transposition $(a\ b)$ and the n-cycle $(1\ 2 \cdots n)$ generate the group S_n if and only if $(a - b, n) = 1$.

An arbitrary p-cycle in S_p can be written as $(1\ 2 \cdots p)$ by relabeling the objects being permuted (that means by applying an overall conjugation on S_p), so to show an arbitrary transposition and p-cycle generate S_p it suffices to show each transposition and the specific p-cycle $(1\ 2 \ldots p)$ generate S_p. For a transposition $(a\ b)$ where $1 \leq a < b \leq p$, we have $(b-a, p) = 1$, so $\langle (a\ b), (1\ 2 \cdots p) \rangle = S_p$ by the fact.

Conclusion. Various kinds of generating sets of some groups are listed below.

Group	Generating Set	Size of Generating Set
$S_n (n \geq 2)$	$(i\ j)$'s	$n(n-1)/2$
	$(1\ 2), (1\ 3), \ldots, (1\ n)$	$n-1$
	$(1\ 2), (2\ 3), \ldots, (n-1\ n)$	$n-1$
	$(1\ 2), (1\ 2 \cdots n)$ if $n \geq 3$	2
	$(1\ 2), (2\ 3 \cdots n)$ if $n \geq 3$	2
	$(a\ b), (1\ 2 \cdots n)$ if $(b-a, n) = 1$	2
$A_n (n \geq 3)$	3-cycles	$n(n-1)(n-2)/3$
	$(1\ i\ j)$'s	$(n-1)(n-2)$
	$(1\ 2\ i)$'s	$n-2$
	$(i\ i+1\ i+2)$'s	$n-2$
	$(1\ 2\ 3), (1\ 2 \cdots n)$ if $n \geq 4$ odd	2
	$(1\ 2\ 3), (2\ 3 \cdots n)$ if $n \geq 4$ even	2
$\mathrm{SL}_2(\mathbb{Z})$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	2
$\mathrm{GL}_n(\mathbb{R}), \mathrm{SL}_n(\mathbb{R})$	Elementary Matrices	∞

24. What is the symmetry group of a tetrahedron? Cube? Icosahedron?

Answer. They are S_4, S_4 (which is exactly $\mathrm{Aut}(Q_8)$; see Set II, Question 13), and S_5, respectively.

25. How many ways can you color the tetrahedron with C colors if we identify symmetric colorings?

Lemma. (Burnside) The number of orbits of G acting on a set X is given by

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|,$$

i.e. the average of invariant elements under the action of G.

Solution. The set X of all paintings of the tetrahedron by up to C different colours has C^4 elements. Two equivalent paintings are differed by a $\sigma \in S_4$. Thus the number of different paintings is the number of orbits in X under the action of the symmetry group of the cube. By Burnside's Lemma,

$$|X/S_4| = \frac{1}{24}(C^4 + 6C^3 + 11C^2 + 6C).$$

26. What is the symmetry group of an icosahedron? What's the stabiliser of an edge? How many edges are there? How do you know the symmetry group of the icosahedron is the same as the symmetry group of the dodecahedron? Do you know the classification of higher-dimensional polyhedra?

27. Do you know what the quaternion group is? How many elements are there of each order?

Answer. By definition, the quaternion group

$$Q_8 := \langle i, j : i^2 = j^2 = -1, iji^{-1} = j^{-1} \rangle.$$

The Q_8 is not a semidirect product, but it is a quotient of a semidirect product. Let $H = \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ with $(a, b)(c, d) = (a + (-1)^b c, b + d)$. Then $(2, 2) \in Z(H)$ has order 2. It turns out that $Q_8 \cong H/\langle (2, 2) \rangle$.

From this, we know Q_8 is generated by two cyclic subgroups of order 4. Say $k = ij$ and there are 6 elements of order 4: $i^{\pm 1}, j^{\pm 1}, k^{\pm 1}$; the only element of order 2 is $i^2 = j^2 = k^2 = -1$.

28. What is the group of unit quaternions topologically? What does it have to do with SO(3)?

Answer. Over $\mathbb{C}$, the group of unit quaternions is given by

$$\{a + bi + cj + dk : a, b, c, d \in \mathbb{C},\ a^2 + b^2 + c^2 + d^2 = 1\}.$$

Topologically, it is homeomorphic to $\mathbb{S}^3 \subset \mathbb{C}^4$. There is a natural surjective homomorphism to SO(3) with kernel $\{\pm 1\}$. There is a short exact sequence

$$1 \to \{\pm 1\} \to \mathbb{S}^3 \to \mathrm{SO}(3) \to 1,$$

meaning that the group of unit quaternions is a double cover of SO(3), i.e. $\mathbb{S}^3$ is a two-sheeted covering space of SO(3).

Remark. The group of unit quaternions can be viewed as Sp(1) or SU(2). In fact, the Lie algebra of Sp(1) is isomorphic to those of SO(3) and SU(2). The mappings between Sp(1), SU(2) and SO(3) are locally isomorphisms since their Lie algebras are isomorphic.

29. What's the stabilizer of a point in the unit disk under the group of conformal automorphisms?

Solution. Denote $\mathbb{D}$ the open unit disk. For any $f \in \mathrm{Aut}(\mathbb{D})$, there are some $\theta \in \mathbb{R}$ and $\alpha \in \mathbb{D}$ such that

$$f(z) = e^{i\theta} \cdot \frac{\alpha - z}{1 - \overline{\alpha} z}, \quad \forall z \in \mathbb{D}.$$

It turns out that the second factor is an involution. For a fixed $z \in \mathbb{D}$ and $\theta \in \mathbb{R}$, we can choose $\alpha = 2e^{-i\theta} z/(1 + |z|^2)$ to get $f(z) = z$. Hence it is parameterized by $\mathbb{S}^1$. In particular, for $z = 0$, we get $f(z) = e^{i\theta}\alpha$ with $\alpha = 0$, for which $e^{i\theta}$ can be chosen arbitrarily on $\mathbb{S}^1$.

30. What group-theoretic construct relates the stabilizers of two points?

Answer. It's conjugate, by definition (since two stabilizers are conjugate to each other).

31. Consider $\mathrm{SL}_2(\mathbb{R})$ acting on $\mathbb{R}^2$ by matrix multiplication. What is the stabiliser of a point? Does it depend which point? Do you know what sort of subgroup this is? What if $\mathrm{SL}_2(\mathbb{R})$ acts by Möbius transformations instead?

    Answer. For example, we may compute

    $$\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{R})}(1,0) = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} : a, b \in \mathbb{R} \right\}$$

    for the fixed point $(1,0)$. Indeed, this is one of Borel subgroups (i.e., the maximal Zariski closed, connected, and solvable algebraic subgroups) of $\mathrm{SL}_2(\mathbb{R})$. Its explicit type depends on the point we choose, but the stabilizer is Borel for all points. $\mathrm{SL}_2(\mathbb{R})$ acts by Möbius transformations on $\mathbb{H}$ by

    $$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \longmapsto \frac{az+b}{cz+d}, \quad \gamma \in \mathrm{SL}_2(\mathbb{R}).$$

32. What are the polynomials in two real variables that are invariant under the action of D_4, the symmetry group of a square, by rotations and reflections on the plane that the two variables form?

    Solution. Consider the action of D_4 on the square with vertices $(\pm 1, 0), (0, \pm i)$ over $\mathbb{C} \cong \mathbb{R}^2$. Since D_4 is generated by two elements $(x,y) \mapsto (y,x)$ and $(x,y) \mapsto (ix, iy)$, the polynomials $f(x,y) \in \mathbb{C}[x,y]$ such that $f(x,y) = f(y,x)$ and $f(x,y) = f(ix,iy)$ are the desired, for example, $x^4 + y^4$ and $(x^2 - y^2)^2$.

33. Give an interesting example of a subgroup of the additive group of the rationals.

    Boring Example. All the rationals with a fixed denominator (and hence this subgroup can be realized as $\mathbb{Z} \hookrightarrow \mathbb{Q}$).

    Interesting Example. The following is an additive subgroup of $\mathbb{Q}$:

    $$H = \{a/b \in \mathbb{Q} : b \neq 0, a + b \equiv 0 \bmod 2\}.$$

    Check that $-a/b \in H$ because of $-a + b = a + b - 2a \equiv 0 \bmod 2$.

34. Talk about the isomorphism classes of subgroups of $\mathbb{Q}$. How many are there? Are the ones you've given involving denominators divisible only by certain primes distinct? So that gives you the cardinality. Are these all of them?

    Answer. There is only one nontrivial isomorphism class for $(\mathbb{Q}, +)$, and the other one is $\{0\}$. To show this, let H, K be two subgroups and h, k be nonzero elements. A group isomorphism can be given by $x \mapsto kx/h$. The class can be represented by any subset S of primes corresponding to $\mathbb{Q}[\frac{1}{S}]$, the set of $\mathbb{Q}$ whose denominators are divisible by no primes outside of S. They are not distinct with intersection $\mathbb{Z}$ involved. These are indeed not all of them.

35. Is the additive group of the reals isomorphic to the multiplicative group of the positive reals? Is the same result true with reals replaced by rationals?

    Answer. Yes, an isomorphism is given by

    $$(\mathbb{R}, +) \to (\mathbb{R}_{>0}, \times), \quad x \mapsto e^x.$$

However, the result does not hold for $\mathbb{Q}$, because $(\mathbb{Q},+)$ contains elements of finite order (i.e. for some $x \in \mathbb{Q}$ we have $nx = 0$ with $n \in \mathbb{N}$), while nontrivial element of $(\mathbb{Q}_{>0}, \times)$ have the infinite order.

36. What groups have nontrivial automorphisms?

    Answer. For example, any non-abelian group has nontrivial inner automorphisms. (An inner automorphism of a group G is $x \mapsto g^{-1}xg$ for $g \in G$. If G is non-abelian, then there exists some $g \in G$ such that $gx \neq xg$ for some $x \in G$.) Another example of a group with nontrivial automorphisms is the cyclic group of order $n > 2$.

37. A subgroup H of a finite group G that meets every conjugacy class is in fact G. Why is that true?

    Proof. Note that
$$N = \bigcap_{g \in G} gHg^{-1}$$
    is the largest normal subgroup of G contained in H. The normality is easy to check. It is the largest because for another $N_0 \lhd G$ such that $N_0 \subset H$, $N_0 = gN_0g^{-1} \subset gHg^{-1}$ for all $g \in G$, and hence $N_0 \subset N$. Since H meets all conjugacy classes, so also does N. But for a normal subgroup, once it contains an element in some conjugacy class, it must involve the whole conjugacy class. Therefore, $N = G \subset H$.

38. Let G be the group of invertible 3×3 matrices over $\mathbb{F}_p$, for p prime. What does basic group theory tell us about G? How many conjugates does a Sylow p-subgroup have? Give a matrix form for the elements in this subgroup. Give a matrix form for the normalizer of the Sylow p-subgroup.

    Answer. For $G = \mathrm{GL}_3(\mathbb{F}_p)$, it has order $(p^3-1)(p^3-p)(p^3-p^2) = p^3(p-1)^3(p+1)(p^2+p+1)$. By Sylow's theorems, there is a Sylow p-subgroup of order p^3 in G, and $n_p \equiv 1 \bmod p$ with $n_p \mid (p-1)^3(p+1)(p^2+p+1)$. It turns out that $n_p = (p+1)(p^2+p+1)$. A Sylow p-subgroup of G, say U, is given by upper triangular matrices with all 1's on the diagonal. The number of conjugacy classes is equal to the index of its normalizer. In fact, the normalizer is $B_n(\mathbb{F}_p)$, the Borel subgroup of all upper triangular invertible matrices. The following argument shows this.

    Addendum. Consider a map $B_n(\mathbb{F}_p) \to B_n(\mathbb{F}_p)$ sending a matrix to a diagonal matrix by simply forgetting other items. This is in fact a homomorphism whose kernel is U, which is normal in $B_n(\mathbb{F}_p)$. Suppose $g \in G$ normalizes U. By Bruhat decomposition $g = b_1wb_2$ for some $b_1, b_2 \in B_n(\mathbb{F}_p)$ and w is a permutation matrix. Since g and b_1, b_2 normalize U, so also does $w = b_1^{-1}gb_2^{-1}$. An easy matrix computation shows that the only permutation matrix normalizing U is I_n. Hence $g = b_1b_2 \in B_n(\mathbb{F}_p)$. On the other hand, we are able to find the order of the normalizer $B_n(\mathbb{F}_p)$ as well as its index in G.

39. Let's look at $\mathrm{SL}_2(\mathbb{F}_3)$. How many elements are in that group? What is its centre? Identify $\mathrm{PSL}_2(\mathbb{F}_3)$ as a permutation group.

    Fact. The projective special linear groups $\mathrm{PSL}_n(\mathbb{F}_q) := \mathrm{SL}_n(\mathbb{F}_q)/Z(\mathrm{SL}_n(\mathbb{F}_q))$ is simple for all $n \geq 2$ and $\mathbb{F}_q$ except for $n = 2$ and $q = 2$ or 3. Indeed,
$$\mathrm{PSL}_2(\mathbb{F}_2) \cong S_3, \quad \mathrm{PSL}_2(\mathbb{F}_3) \cong A_4,$$
    which are not simple but can be easily computed.

Solution. By multiplicating -1 on the first row of any element in $\mathrm{SL}_2(\mathbb{F}_3)$, its determinant changes. This gives a bijection between those whose respective determinants are 1 and -1 in $\mathrm{GL}_2(\mathbb{F}_3)$. Therefore,

$$|\mathrm{SL}_2(\mathbb{F}_3)| = \frac{1}{2}|\mathrm{GL}_2(\mathbb{F}_3)| = \frac{(3^2-1)(3^2-3)}{2} = 24.$$

In the sense of "projective", it is easy to check the center is given by those scalar matrices, i.e., $Z(\mathrm{SL}_2(\mathbb{F}_3)) \cong \mathbb{F}_3^\times$.

40. How many elements does $\mathrm{GL}_2(\mathbb{F}_q)$ have? How would you construct representations? What can you say about the 1-dimensional representations? What can you say about simplicity of some related groups?

Answer. There are $(q^2-1)(q^2-q)$ elements together with $(q-1)(q+1)$ conjugacy classes in $\mathrm{GL}_2(\mathbb{F}_q)$ (see Question 21 in Set IV). The representations of $\mathrm{GL}_2(\mathbb{F}_q)$ can be classified as follows.

Type	Example	Size	Representation
central	$\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$	$q-1$	1-dimensional
non-semisimple	$\begin{pmatrix} x & 1 \\ 0 & x \end{pmatrix}$	$q-1$	special
split semisimple	$\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$	$(q-1)(q-2)/2$	regular principal series
anisotropic semisimple	$\begin{pmatrix} * & * \\ * & * \end{pmatrix}$	$(q^2-q)/2$	supercuspidal

Recall that "anisotropic" denotes the conjugacy classes whose eigenvalues lies properly in a (unique) quadratic extension of $\mathbb{F}_q$, and with Galois norm 1.

41. A subgroup of a finitely-generated free abelian group is? A subgroup of a finitely-generated free group is? Prove your answers.

Proposition. Let F be a free abelian group of rank n and H be a subgroup. Then there exists a basis $\{f_1, \dots, f_n\}$ of F and integers $d_1, \dots, d_r \in \mathbb{N}$ with $r \leq n$ such that $d_i \mid d_{i+1}$ and

$$\{d_1 f_1, \dots, d_r f_r\}$$

is a basis of H as a free abelian subgroup.

Theorem. (Nielsen–Schreier) Every subgroup of H of a free group F is free.

Answer. In the free case, it is free as well and is generated by fewer generators. In the non-free case, it is free with unbounded generators.

Proof Idea. Consider covering spaces of a wedge product of loops. Note that finitely generated torsion free abelian implies free abelian.

42. What are the subgroups of $\mathbb{Z}^2$?

Answer. The question can be considered geometrically by viewing $\mathbb{Z}^2$ a full lattice of $\mathbb{C}$. Granting this, all subgroups of $\mathbb{Z}^2$ are generated by pairs of vectors (a, b) and (c, d) with $a, b, c, d \in \mathbb{Z}$. The index of such subgroup is $|ad - bc|$.

43. What are the subgroups of the free group F_2? How many generators can you have? Can you find one with 3 generators? 4 generators? Countably many generators? Is the subgroup with 4 generators you found normal? Why? Can you find a normal one?

    Answer. By definition, F_2 is generated by the words consisting of two non-commutative elements a, b with a^{-1}, b^{-1}. The subgroups of F_2 can be of any countable rank because there are countably infinitely many independent generators in F_2 to choose. An arbitrarily chosen subgroup is not necessarily normal, but we can take the normal closure to remedy this.

44. Talk about the possible subgroups of $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$. Now suppose that you have a subgroup of $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$. What theorem tells you something about the structure of the quotient group?

    Answer. Like Question 42, any subgroup of $\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$ is free and abelian of rank at most 3. Every group can be expressed as the quotient of a free group by a normal subgroup. Hence the quotient group can be essentially generated by at most 3 elements, and can have torsion structures.