# 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 $G = G_0 \geqslant G_1 \geqslant \cdots \geqslant G_n = 1$, where each $G_i/G_{i+1}$ is abelian. $S_4$ is nonabelian but solvable, because $S_4 \triangleright A_4 \triangleright K \triangleright 1$, 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 $G = G_0 \geqslant G_1 \cdots \geqslant G_n \geqslant \cdots$, where $G_{i+1} = [G, G_i] = [G_i, G]$. Upper central series is $1 = Z_0 \leqslant Z_1 \leqslant Z_2 \leqslant \ldots \leqslant Z_n \leqslant \ldots$, 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 $H^{(i)} \leqslant G^{(i)}$.

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 $\mu_{12}$.

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 $\rho$ with character $\chi$, 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,

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

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

*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 $n \geqslant 5$ 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

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

    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 $1 \leqslant i \leqslant r$.

    *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 $H \leqslant G$ 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 $m \leqslant n$. 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 $\sigma$ in it must commute with all transpositions. Since $\sigma$ has order at least 2, a non-disjoint transposition gives the contradiction.

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

*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 $n \geqslant 3$.

*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 $\sigma$ 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 $1 \leqslant a < b \leqslant n$, 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 $1 \leqslant a < b \leqslant p$, 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 |
|---|---|---|
| $S_n (n \geqslant 2)$ | $(i\ j)$'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 $n \geqslant 3$ | 2 |
| | $(1\ 2), (2\ 3\cdots n)$ if $n \geqslant 3$ | 2 |
| | $(a\ b), (1\ 2\cdots n)$ if $(b-a, n) = 1$ | 2 |
| $A_n (n \geqslant 3)$ | 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 $n \geqslant 4$ odd | 2 |
| | $(1\ 2\ 3), (2\ 3\cdots n)$ if $n \geqslant 4$ 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 | $\infty$ |

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 $\mathbb{Q}$:

$$H = \{a/b \in \mathbb{Q} : b \neq 0, a \equiv 0 \bmod 2, (a, b) = 1\}.$$

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 $N_0 \triangleleft G$ 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 $3 \times 3$ 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 $n \geqslant 2$ 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 $\{f_1, \ldots, f_n\}$ of $F$ and integers $d_1, \ldots, d_r \in \mathbb{N}$ with $r \leqslant n$ such that $d_i \mid d_{i+1}$ and

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

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.

## 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

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

   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

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

   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

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

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 $\operatorname{Syl}_p(G)$ by conjugation:

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

The fixed points are $\{Q \in \operatorname{Syl}_p(G) : pQp^{-1} = Q, \forall p \in P\}$. 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 $\operatorname{Syl}_p(G)$ 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,

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

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

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

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 $n_p = n_q = 1$ (see Question 5 below). 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 $q \equiv 1 \bmod p$ necessarily has two possible 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

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

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 $n_7 = 1$. 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 preceding 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 $n \geqslant 4$

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

  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 $200=2^3\cdot5^2$, 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 $|G|=132=2^2\cdot3\cdot11$. Then $n_{11}\equiv1 \bmod 11$ and $n_{11}\mid12$, which implies $n_{11}=12$ by assumption (otherwise $n_{11}=1$ and $N_{11}$ is a normal subgroup). By Sylow again together with $n_3\neq1$, it turns out to be $n_3\geqslant4$. 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 $160=2^5\cdot5$ 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 $p^aq^b$ 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.

## Set III: Fields and Galois Theory

1. What is the Galois group of a finite field? What is a generator? How many elements does a finite field have? What can you say about the multiplicative group? Prove it.

   *Answer.* Consider $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^r})$ for $r \mid n$ corresponding to an irreducible polynomial of degree $f = n/r$ over $\mathbb{F}_{p^r}$. It is cyclic of order $f$ with generator $\mathrm{Frob}_p$.

   *Claim.* For a finite field $F = \mathbb{F}_{p^d}$, $F^\times = F - \{0\} \cong \mathbb{Z}/(p^d - 1)\mathbb{Z}$ is cyclic.

   *Proof.* Elements of $\mathbb{F}_{p^d}$ are roots of $x^{p^d} - 1$. So each invertible element has a $p$-power order. But $\mathrm{Frob}_p$ acts transitively on these roots, so there is only one generator of $F^\times$ whose order is $p^d - 1$.

   *Warning.* We are morally able to realize $\mathbb{Z}/p\mathbb{Z}$ as $\mathbb{F}_p$. Yet it fails for $\mathbb{F}_{p^d}$.

2. Classify finite fields, their subfields, and their field extensions. What are the automorphisms of a finite field?

   *Answer.* All finite fields are of the form $\mathbb{F}_{p^d}$ with a prime power size. All finite extensions are $\mathbb{F}_{p^m}/\mathbb{F}_{p^d}$ where $d \mid m$. Taking $g$ as the generator of the cyclic group $\mathbb{F}_{p^d}^\times$, then all automorphism $\sigma : \mathbb{F}_{p^d} \to \mathbb{F}_{p^d}$ fixes $g$. This implies that all automorphism are powers of some multiple of $p$.

3. Take a finite field extension $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. What is Frobenius? What is its characteristic polynomial?

   *Answer.* The Frobenius map is $\mathrm{Frob}(x) = x^p$, which is independent of $n$. Since $\mathbb{F}_{p^n}$ is the splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$, we have $\mathrm{Frob}^n - 1 = 0$. Note that this extension is of degree $n$, then $X^n - 1$ is the characteristic polynomial.

4. What is the minimal polynomial of the Frobenius automorphism?

   *Answer.* All elements of $\mathbb{F}_{p^n}$ should be zeroes of the minimal polynomial since it is the splitting field. Thus, the minimal polynomial is the same as the characteristic polynomial $X^n - 1$.

5. What's the field with 25 elements?

   *Answer.* It is of the form $\mathbb{F}_5[x]/(\pi(x))$, where $\pi(x)$ is an irreducible polynomial over $\mathbb{F}_5$ of degree 2, such as $\pi(x) = x^2 - 2$, which is irreducible modulo 5 (but it is not because $\pi$ is Eisenstein at 2).

6. What is the multiplicative group of $\mathbb{F}_9$?

   *Answer.* For a finite field $F$, $F^\times = F - \{0\}$. In $\mathbb{F}_9$, it is a cyclic group of order 8.

7. What is a separable extension? Can $\mathbb{Q}$ have a non-separable extension? How about $\mathbb{Z}/p\mathbb{Z}$? Why not? Are all extensions of characteristic 0 fields separable? Of finite fields? Prove it. Give an example of a field extension that's not separable.

   *Note.* Every algebraic extension of a perfect field is automatically separable. Because every minimal polynomial should be irreducible, and hence separable over perfect fields. Recall the definition of perfectness in Question 9.

   *Answer.* Say $E/F$ is a separable extension if for all $\alpha \in E$, the minimal polynomial of $\alpha$ over $F$ is separable, i.e. it has no multiple roots.

Since $\mathbb{Q}$ and $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ are perfect fields, there are no non-separable extensions over them. So do fields of characteristic 0 and finite fields such that $(\mathbb{F}_q)^p = \mathbb{F}_q$ for $q = p^r$.

*Example.* Consider the non-perfect function field $\mathbb{F}_p(u^p)$ who has an extension $\mathbb{F}_p(u)$. The minimal polynomial of $u$ is $x^p - u^p = (x-u)^p$ since we are working with the characteristic $p$. Hence $\mathbb{F}_p(u)/\mathbb{F}_p(u^p)$ is a non-separable extension.

8. Are there separable polynomials of any degree over any field?

   *Answer.* No. Over perfect fields, this should be valid. But for non-perfect fields of characteristic $p$, a polynomial in $x^p$ is always inseparable because it has zero derivative: see, for example, $\mathbb{F}_p(u^p)$, in Question 7.

9. What is a perfect field and why is this important? Give an example of a non-perfect field.

   *Answer.* It is a field such that every irreducible polynomial is separable. A field $F$ is perfect if and only if $\operatorname{char} F = 0$ or $\operatorname{char} F = p$ and $F^p = F$. Equivalently, every finite extension of $F$ is separable. In particular, all finite fields are perfect. The perfect fields are important because all algebraic extensions above them are separable. See this in Question 7.

   *Example.* The function field $\mathbb{F}_p(u)$ is not perfect. Since $x^p - u$ is irreducible (Eisenstein at $u$) but $(x^p - u)' = px^{p-1} = 0$, which is not separable.

10. What is Galois theory? State the main theorem. What are the intermediate extensions? Which extensions are normal, which are not, and why? What are the Galois groups (over $\mathbb{Q}$) of all intermediate extensions?

    *Statement.* Let $K/F$ be a finite Galois extension with $G := \operatorname{Gal}(K/F)$.

    (1) There is a 1-1 correspondence:

    $$\begin{aligned} \{\text{Subgroups } H \geqslant G\} &\longleftrightarrow \{\text{Intermediate fields } K/L/F\} \\ H &\longmapsto K^H = \{x \in K : h(x) = x,\ \forall h \in H\} \\ \operatorname{Gal}(K/L) &\longleftarrow\!\shortmid L. \end{aligned}$$

    (2) The correspondence is inclusion-reversive:

    $$H_1 \subset H_2 \Longleftrightarrow K^{H_1} \supset K^{H_2}, \quad \#H = [K : K^H], \quad [G : H] = [K^H : F].$$

    (3) The correspondence is acted by conjugations: under conjugation,

    $$H \longleftrightarrow L \quad \Longrightarrow \quad gHg^{-1} \longleftrightarrow g(L).$$

    (4) The correspondence is normal-to-normal:

    $$H \triangleleft G \text{ normal subgroup} \quad \Longleftrightarrow \quad K^H/F \text{ normal extension.}$$

    (5) If $H_1, H_2 \leftrightarrow K_1, K_2$, then

    $$H_1 \cap H_2 \longleftrightarrow K_1K_2; \quad \langle H_1, H_2\rangle \longleftrightarrow K_1 \cap K_2.$$

11. What is a Galois extension?

    *Definition.* A normal and separable extension, i.e., the splitting field of some polynomial over the base field.

12. Take a quadratic extension of a field of characteristic 0. Is it Galois? Take a degree 2 extension on top of that. Does it have to be Galois over the base field? What statement in group theory can you think of that reflects this?

    *Answer.* The quadratic extension should be Galois whereas the composition of quadratic extensions is not necessarily Galois. A counterexample is $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$.

    The separability is transitive under compositions, but Galois property and normality are not. In group theory, normality is neither transitive: consider

    $$\{(1)\} \triangleleft \mathbb{Z}/2\mathbb{Z} \triangleleft V = (\mathbb{Z}/2\mathbb{Z})^2 \triangleleft A_4 \triangleleft S_4,$$

    where our $\mathbb{Z}/2\mathbb{Z}$ is not normal in $A_4$ or $S_4$.

13. Is abelian Galois extension transitive? That is, if $K$ has abelian Galois group over $E$, $E$ has abelian Galois group over $F$, and $K$ is a Galois extension of $F$, is it necessarily true that $\mathrm{Gal}(K/F)$ is also abelian? Give a counterexample involving number fields as well as one involving function fields.

    *Answer.* No. The upshot is read as the semidirect product of abelian groups is not necessarily abelian.

    *Counterexample.* Over number fields, let's consider

    $$\mathbb{Q} \subset \mathbb{Q}(\omega) \subset \mathbb{Q}(\sqrt[3]{2}, \omega).$$

    One can check $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) = S_3 \cong \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ is not abelian. Yet its two Galois subgroups are abelian. Since function fields are very similar to number fields, the same construction works:

    $$\mathbb{F}_p(u) \subset \mathbb{F}_{p^2}(u) \subset \mathbb{F}_{p^2}(u^{1/3}).$$

    This tower has the total Galois group $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ as well, which can be non-abelian.

    *Remark.* The compositum in this case is always abelian. It turns out that if $L_1/K$ and $L_2/K$ are Galois over $K$, there exists a natural injective homomorphism

    $$\begin{aligned} \mathrm{Gal}(L_1L_2/K) &\longrightarrow \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K) \\ \sigma &\longmapsto (\sigma|_{L_1}, \sigma|_{L_2}). \end{aligned}$$

    In particular, if both $L_1/K$ and $L_2/K$ are abelian, then so is $L_1L_2/K$.

14. Talk about the Kummer extension.

    *Theorem.* (Kummer Theory) For any field $K$, define the Kummer pairing as

    $$\langle \cdot, \cdot \rangle : \mathrm{Gal}(\overline{K}/K) \times K^\times \to \{1, \zeta_n, \ldots, \zeta_n^{n-1}\}.$$

    Then there is an isomorphism induced by the pairing, say

    $$K^\times/(K^\times)^n \simeq \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), \mathbb{Z}/n\mathbb{Z}).$$

    *Answer.* The Kummer theory can be expressed through a natural language, say the following two types of objects are in the one-to-one correspondence:

(i) Galois extensions of $K$ with Galois group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^r$.

(ii) Subgroups of $K^\times/(K^\times)^n$ that are isomorphic to $(\mathbb{Z}/n\mathbb{Z})^r$.

In particular, we suppose $r = 1$. If $\zeta_n \in K$, then every $\mathbb{Z}/n\mathbb{Z}$-extension of $K$ is of the form $K(\alpha^{1/n})$ for some $\alpha \in K^\times$ with the property that $\alpha^{1/d} \notin K$ for any proper divisor $d$ of $n$, and vice versa.

15. Say you have a field extension with only finitely many intermediate fields. Show that it is a simple extension.

*Proof.* Let $L/K$ be such an extension. If $L$ is an algebraic extension, then $L$ is simple by primitive element theorem. Suppose there is a transcendental generator $x \in L$ over $K$. Then $K \subset K(x^n) \subset K(x) \subset L$. When $n$ runs through $\mathbb{N}$, we have infinitely many intermediate fields, which leads to a contradiction.

16. Tell me a condition on the Galois group which is implied by irreducibility of the polynomial. What happens when the polynomial has a root in the base field?

*Answer.* The Galois group is transitive if and only if the polynomial is irreducible. When the polynomial has a root in the base field, the root can be dropped and nothing will happen.

17. What is the discriminant of a polynomial?

*Answer.* By definition, $\operatorname{disc} f = \prod_{i<j}(r_i - r_j)^2$, where $r_1, \ldots, r_n$ are all roots of $f$ over its splitting field. Moreover, if $f \in K$ is irreducible of degree $m$, than

$$\operatorname{disc} f = \prod_{1\leqslant i<j\leqslant n} (r_i - r_j)^2 = (-1)^{m(m-1)/2} \operatorname{Nm}_{L/K} f'(\alpha),$$

where $\alpha$ is a simple root of $f$ in its splitting field $L$.

18. If we think of the Galois group of a polynomial as contained in $S_n$, when is it contained in $A_n$?

*Answer.* This happens for $f \in K[T]$ if and only if $\operatorname{disc} f$ is a square in $K$.

*Proof.* For $\delta = \prod_{i<j}(r_i - r_j)$ and $\sigma \in \operatorname{Gal}(f) = \operatorname{Gal}(K(r_1, \ldots, r_n)/K)$, we have

$$\sigma(\delta) = \prod_{i<j}(\sigma(r_i) - \sigma(r_j)) = \varepsilon_\sigma \prod_{i<j}(r_i - r_j) = \varepsilon_\sigma \delta = \pm\delta.$$

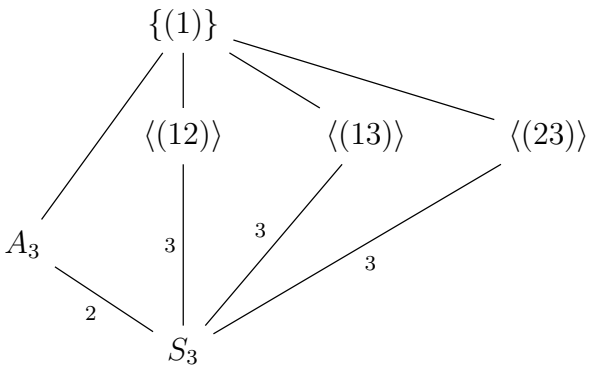
Thus $\sigma \in A_n$ iff $\varepsilon_\sigma = 1$, iff $\sigma(\delta) = \delta$ or $\delta \in K$. This is equivalent to $\operatorname{disc} f = \delta^2 \in K$ is a square in $K$.

19. Is $\mathbb{Q}(\sqrt[3]{2})$ normal? What is its splitting field? What is its Galois group? Draw the lattice of subfields.

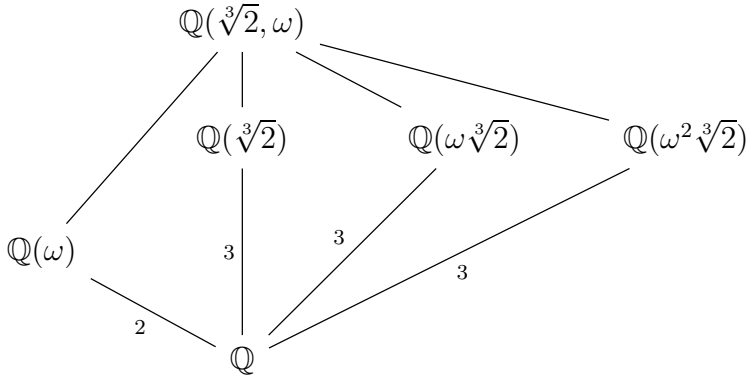
*Answer.* No, the splitting field is $\mathbb{Q}[x]/(x^3 - 2) = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$. For this,

$$\operatorname{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}) = \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong A_3 \rtimes \mathbb{Z}/2\mathbb{Z} = S_3.$$

The lattice of subgroups:




This deduces the lattice of subfields:




20. What is the Galois group of $x^2+1$ over $\mathbb{Q}$? What is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(i)$?

    *Solution.* The splitting field is $\mathbb{Q}(i)$ and the Galois group is $\{1, c\}$, where $c$ is the complex conjugate. Here $d = -1 \equiv 3 \bmod 4$, hence the integral closure of $\mathbb{Z}$ is $\mathbb{Z}[i]$.

21. What's the Galois group of $x^2+9$?

    *Solution.* The splitting field is $\mathbb{Q}(\sqrt{-3})$ with the Galois group $\{1, c\}$.

22. What is the Galois group of $x^2-2$ over $\mathbb{Q}$? Why is $x^2-2$ irreducible?

    *Solution.* The Galois group is $\mathbb{Z}/2\mathbb{Z} \cong \{1, r\}$ where $r$ swaps $\pm\sqrt{2}$, and $x^2-2$ is irreducible over $\mathbb{Q}$ since it is Eisenstein at 2.

23. What is the Galois group of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}$?

    *Solution.* It is $\mathbb{Z}/2\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} = (\mathbb{Z}/2\mathbb{Z})^2 \cong \{1, r, s, rs\}$ where $r$ swaps $\pm\sqrt{2}$ and $s$ swaps $\pm\sqrt{3}$ (note that $\mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/2\mathbb{Z}) = 1$ is always trivial). It embeds into $S_4$ by, for example, $\{(1), (12), (34), (12)(34)\}$.

24. What is the Galois group of $\mathbb{Q}(\sqrt{n_1},\sqrt{n_2},\ldots,\sqrt{n_m})$ over $\mathbb{Q}(\sqrt{n_1}+\ldots+\sqrt{n_m})$?

    *Solution.* It is trivial. May assume all $n_i$ are mutually distinct and square-free. Then each Galois action sends each $\sqrt{n_i}$ to either $\sqrt{n_i}$ or $-\sqrt{n_i}$. Here comes $2^m$ Galois actions. On the other hand, $\sqrt{n_1}+\cdots+\sqrt{n_m}$ also has an orbit of size $2^m$, say $\{\pm\sqrt{n_1}\pm\cdots\pm\sqrt{n_m}\}$. Hence these two fields are equal.

25. What are the Galois groups of irreducible cubics?

    *Answer.* Isomorphic to $A_3$ (otherwise, $S_3$) if disc $f$ is a square in $K$, where char $K \neq 2$.

    *Proof.* Just because $\mathrm{Gal}(f) = \mathrm{Gal}(K(r_1, r_2, r_3)/K)$ (being transitive by irreducibility) embeds into $S_3$ and its order is divisible by $[K(r_i) : K] = 3$. So $\mathrm{Gal}(f) = S_3$ or $A_3$. Then apply Question 18.

26. If an irreducible cubic polynomial has Galois group NOT contained in $A_3$, does it necessarily have to be all of $S_3$?

    *Answer.* Yes, for char $K \neq 2$. See Question 25.

27. Compute the Galois group of $x^3 - 2$ over the rationals.

    *Solution.* Apply Question 25. $x^3 - 2$ is irreducible (Eisenstein at 2) with disc $= -4a^3 - 27b^2 = -108 \neq \square$ in $\mathbb{Q}$. Hence it is $S_3$.

28. How would you find the Galois group of $x^3 + 2x + 1$? Adjoin a root to $\mathbb{Q}$. Can you say something about the roots of $x^3 + 3x + 1$ in this extension?

    *Solution.* Since $x^3 + 2x + 1$ is irreducible modulo 3, it is irreducible over $\mathbb{Q}$. Note that $\mathrm{disc}(x^3 + 2x + 1) = -59 \neq \square$, it has a Galois group $S_3$.

    *Answer.* The splitting fields of both $x^3 + 2x + 1$ and $x^3 + 3x + 1$ are of degree 6 since both are irreducible polynomials over $\mathbb{Q}$. They are either equal or disjoint. Also, they are equal if and only if their discriminants are differed by some perfect square (i.e. both splitting fields contain the same $\mathbb{Q}(\sqrt{\Delta})$). However, $\mathrm{disc}(x^3 + 3x + 1) = -135$. So none of the roots of $x^3 + 3x + 1$ lie in $\mathbb{Q}[x]/(x^3 + 2x + 1)$.

    *Key Features.* Since the discriminant is a symmetric polynomial of all roots, if $f \in \mathbb{Q}[x]$ is a polynomial with discriminant $\Delta$, then $\mathbb{Q}(\sqrt{\Delta}) \subset \mathbb{Q}[x]/(f(x))$, containing in the splitting field.

29. Compute the Galois group of $x^3 + 6x + 3$.

    *Solution.* Apply Question 25: $x^3 + 6x + 3$ is irreducible (Eisenstein at 3) with disc $= -1107 \neq \square$ in $\mathbb{Q}$. Hence it is $S_3$.

30. Find the Galois group of $x^4 - 2$ over $\mathbb{Q}$.

    *Solution.* The splitting field is $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ with degree 8. And

    $$\mathrm{Gal}(f) \cong \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong D_4.$$

31. What's the Galois group of $x^4 - 3$?

    *Solution.* Similar to Question 30. The answer is $D_4$.

32. What is the Galois group of $x^4 - 2x^2 + 9$?

    *Solution.* This is irreducible over $\mathbb{Q}$ since it is irreducible modulo 5. It has discriminant $186192 = 2^4 \times 3^3 \times 431$ and cubic resolvent $R_3(x) = x^3 - 36x - 4$. Since $R_3(x + 1) = x^3 + 3x^2 - 33x - 39$ is Eisenstein at 3, it is irreducible. Hence $\mathrm{Gal}(f) = S_4$ by the following recipe.

    *Recipe.* Here is a general recipe to compute Galois groups of irreducible quartics over $K$ whose characteristics are not 2:

| $\operatorname{disc} f$ in $K$ | $R_3(X)$ in $K[X]$ | $\mathrm{Gal}(f)$ |
|---|---|---|
| $\neq \square$ | irreducible | $S_4$ |
| $= \square$ | irreducible | $A_4$ |
| $\neq \square$ | reducible | $D_4$ or $\mathbb{Z}/4\mathbb{Z}$ |
| $= \square$ | reducible | $V$ |

The cubic resolvent is given by

$$R_3(X) = (X - (r_1r_2 + r_3r_4))(X - (r_1r_3 + r_2r_4))(X - (r_1r_4 + r_2r_3)).$$

In particular, when $f(x) = x^4 + cx + d$, we get $R_3(x) = x^3 - 4dx - c^2$. Also recall that $\operatorname{disc}(x^4 + cx + d) = -27c^4 + 256d^3$.

33. Calculate the Galois group of $x^5 - 2$.

*Solution.* Note that $\mathbb{Q}[x]/(x^5 - 2) = \mathbb{Q}(\zeta_5, \sqrt[5]{2})$. Then

$$\mathrm{Gal}(\mathbb{Q}(\zeta_5, \sqrt[5]{2})/\mathbb{Q}) = \mathbb{Z}/5\mathbb{Z} \rtimes_\varphi \mathbb{Z}/4\mathbb{Z},$$

where $\varphi : \mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z}) \cong \mathbb{Z}/4\mathbb{Z}$ is nontrivial but unique.

34. Discuss sufficient conditions on a polynomial of degree 5 to have Galois group $S_5$ over $\mathbb{Q}$ and prove your statements.

*Answer.* The sufficient conditions can be various. We let the irreducible polynomial have exactly 3 real roots and a pair of complex roots. By labeling these roots $\{1, 2, 3, 4, 5\}$, our condition leads to the existence of a transposition and a 3-cycle in Galois group. However, a transitive subgroup of $S_n$ that contains a transposition and a $p$-cycle with $p > n/2$ can only be $S_n$ itself.

35. Show that if $f$ is an irreducible quintic with precisely two nonreal roots, then its Galois group is $S_5$.

*Proof.* In the conclusion of Question 23 of Set I, we see $S_n$ can be generated by $(a\ b)$ and $(1\ 2 \cdots n)$ if $(b - a, n) = 1$. In this case, as $f$ has a couple of conjugate complex roots, there exists some prime $p$ such that $f(x) \equiv f_3(x)f_2(x) \bmod p$, where $\deg f_2 = 2$ is irreducible over $\mathbb{F}_p$ and $\deg f_3 = 3$. Then (possibly after permuting the roots of $f$ when necessary), $\mathrm{Gal}(f)$ contains $(1\ 2\ 3)$ and $(4\ 5)$. Consequently, $\mathrm{Gal}(f) = S_5$.

36. Suppose you have a degree 5 polynomial over a field. What are necessary and sufficient conditions for its Galois group to be of order divisible by 3? Can you give an example of an irreducible polynomial in which this is not the case?

*Answer.* The Galois group has order divisible by 3 if and only if it contains an element of order 3, namely a 3-cycle. Equivalently, there is some prime $p$ such that $f(x) \bmod p$ has an irreducible factor of degree 3.

*Example.* Let $f(x) = x^5 + ax + b \in \mathbb{Q}[x]$. Then $\mathrm{Gal}(f) \cong D_5$ if and only if:

(i) $f(x)$ is irreducible over $\mathbb{Q}$;

(ii) $\operatorname{disc}(f(x)) = 4^4a^5 + 5^5b^4 = \square$ is a perfect square;

(iii) $f(x)$ is solvable by radicals.

37. What is the Galois group of $x^7 - 1$ over the rationals?

*Solution.* See Question 38 below. It's $(\mathbb{Z}/7\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z}$.

38. What is the Galois group of the polynomial $x^n - 1$ over $\mathbb{Q}$?

*Answer.* We have $\mathbb{Q}[x]/(x^n - 1) = \mathbb{Q}(\zeta_n)$ and an isomorphism

$$\begin{aligned}(\mathbb{Z}/n\mathbb{Z})^\times &\longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \\ k \bmod n &\longmapsto \sigma_k,\end{aligned}$$

where $\sigma_k(x) = x^k$.

39. Describe the Galois theory of cyclotomic extensions.

*Answer.* Same as Question 38. Note that one can use Kronecker–Weber theorem to determine the abelian extension (in explicit description) for a given cyclic Galois group.

40. What is the maximal real field in a cyclotomic extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$?

*Answer.* It's $M = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Since $\mathbb{Q}(\zeta_n)$ is not totally real, we have $[\mathbb{Q}(\zeta_n) : M] \geqslant 2$. This morally equal to 2: convert $\mathbb{Z}/2\mathbb{Z}$ into a multiplicative group $\{\pm 1\}$, which fixes

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/M}(\zeta_n) = \zeta_n + \zeta_n^{-1}.$$

*Remark.* The intrinsic fact we've used here is $\varphi(n)$ being even for all $n \geqslant 3$.

41. Compute the Galois group of $p(x) = x^7 - 3$.

*Answer.* The splitting field is $\mathbb{Q}(\sqrt[7]{3}, \zeta_7)$. Hence

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[7]{3}, \zeta_7)/\mathbb{Q}) = \mathbb{Z}/7\mathbb{Z} \rtimes_\varphi \mathbb{Z}/6\mathbb{Z},$$

where $\varphi : \mathbb{Z}/6\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/7\mathbb{Z}) \cong \mathbb{Z}/6\mathbb{Z}$ is nontrivial but unique.

42. What Galois stuff can you say about $x^{2^n} - 2$?

*Answer.* Recall that

$$\mathrm{disc}(x^k + a) = (-1)^{k(k-1)/2} k^k a^{k-1}.$$

Then $\mathrm{disc}(x^{2^n} - 2) = -2^{(n+1)\cdot 2^n} \neq \square$ for any $n \geqslant 2$. The splitting field is $\mathbb{Q}(\zeta_{2^n}, 2^{2^{-n}})$, and the Galois group is $\mathbb{Z}/2^n\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z})$ when $n > 2$.

43. What are the cyclic extensions of (prime) order $p$?

*Answer.* By Kronecker–Weber, it is a subfield $F$ of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ for some integer $n$ such that $p \mid \varphi(n)$. Say $\varphi(n) = kp$ and $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times \cong \mathbb{Z}/\varphi(n)\mathbb{Z}$ who has a subgroup $\mathbb{Z}/k\mathbb{Z} \cong \mathrm{Gal}(\mathbb{Q}(\zeta_n)/F)$. This subgroup has image $\langle x \rangle \subset \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ such that $x^k = 1$ in $(\mathbb{Z}/n\mathbb{Z})^\times$ under multiplication. Then

$$F = \mathbb{Q}(\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/F}(\zeta_n)) = \mathbb{Q}(\zeta_n + \zeta_n^x + \cdots + \zeta_n^{x^{k-1}}).$$

*Caution.* This question is not asking for cyclotomic extensions $\mathbb{Q}(\zeta_p)$. But recall that $\mathbb{Q}(\zeta_p)$ is the smallest extension generated by Kronecker–Weber that contains $\mathbb{Q}(\sqrt{p^*})$, where $p^* = (-1)^{(p-1)/2}p$; namely, $p$ is the conductor of $\mathbb{Q}(\sqrt{p^*})$. This fact relates to the quadratic reciprocity.

44. Can you give me a polynomial whose Galois group is $\mathbb{Z}/3\mathbb{Z}$?

    *Answer.* Any irreducible cubic whose discriminant is a square. For example, $x^3-3x-1$ with disc $= 81$, whose roots are $r, r^2-r-2, -r^2+2$.

45. Which groups of order 4 can be realised as a Galois group over $\mathbb{Q}$?

    *Answer.* Both of them: for square-free integers $m \neq n$,

    $$\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}, \quad \mathrm{Gal}(\mathbb{Q}(\sqrt{m},\sqrt{n})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

46. Give a polynomial with $S_3$ as its Galois group.

    *Answer.* It must be an irreducible cubic whose discriminant is not a rational square.

47. How do you construct a polynomial over $\mathbb{Q}$ whose Galois group is $S_n$? Do it for $n = 7$ in particular.

    *Key Tool.* For $n \geqslant 2$, let $H$ be a transitive subgroup of $S_n$. If one of the followings are valid, then $H = S_n$:

    - $H$ contains a 2-cycle (i.e., a transposition) and a $p$-cycle ($p > n/2$),
    - $H$ contains a 2-cycle and a $(n-1)$-cycle, or
    - $n \geqslant 3$, $H \neq A_n$ contains a 3-cycle and a $p$-cycle ($p > n/2$).

    *Answer.* We need to find an irreducible polynomial of degree 7 who has a degree 2 factor mod $p_1$ (and hence a 2-cycle) together with a degree 6 factor mod $p_2$ (and hence an $(n-1)$-cycle) for some primes $p_1$ and $p_2$. Let $f(X) = X^7 - X - 1$. The first few factorizations of $f(X)$ mod $p$ are as follows:

    $$\begin{aligned} f(X) &\equiv X^7 + X + 1 \bmod 2, \\ f(X) &\equiv (X^2 + X + 2)(X^5 + 2X^4 + 2X^3 + 2X + 1) \bmod 3, \\ f(X) &\equiv (X+3)(X^6 + 2X^5 + 4X^4 + 3X^3 + X^2 + 2) \bmod 5. \end{aligned}$$

    So $f(X)$ is in need.

48. What's a Galois group that's not $S_n$ or $A_n$?

    *Answer.* It's in general a composition of series of semidirect products of cyclic groups. A quartic extension may have Galois group $V = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $D_4 = \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

49. Which finite groups are Galois groups for some field extension?

    *Answer.* The following theorem by Artin shows that each finite group can be realized as a Galois group: given a field $K$ and let $G \leqslant \mathrm{Aut}(K)$; then $K/K^G$ is a Galois extension with Galois group $G$.

    Under this assumption, let $F$ be an arbitrary field and adjoin all $g \in G$ as transcendental elements into $F$ to get $L = F(g_1, \dots g_n)$, where $n = |G|$. Note that any action of $G$ on $L$ gives a multiplication over generators, so $G$ embeds into $\mathrm{Aut}(L)$. This shows that $\mathrm{Gal}(L/L^G) = G$.

50. What Galois group would you expect a cubic to have?

    *Answer.* Suppose the cubic is irreducible and then the Galois group is transitive. Since we get an intermediate field by adding only one root, the Galois group is a subgroup with order divisible by 3. Hence it's $A_3$ or $S_3$.

51. Draw the subgroup lattice for $S_3$.

*Answer.* There are 3 subgroups of index 3; only $A_3$ has index 2. See Question 19.

52. Do you know what the quaternion group is? How many elements are there of each order? Suppose I have a field extension of the rationals with Galois group the quaternion group. How many quadratic extensions does it contain? Can any of them be imaginary?

*Answer.* For the quaternion group, see Question 27 in Set I. There are 3 different quadratic extensions, say $\mathbb{Q}(\sqrt{a})$, $\mathbb{Q}(\sqrt{b})$, and $\mathbb{Q}(\sqrt{a},\sqrt{b})$. Note that at least one of them is totally real.

A theorem of Witt asserts that a biquadratic extension $F(\sqrt{a},\sqrt{b}), a, b \in F^\times$ can be embedded in a quaternion Galois extension of $F$ iff the quadratic form $ax^2+by^2+abz^2$ is isomorphic over $F$ to $x^2+y^2+z^2$. For $F=\mathbb{Q}$ this forces $a, b, ab > 0$. Hence all of them cannot be imaginary.

53. Suppose you are given a finite Galois extension $K/\mathbb{Q}$ by $f(x) \in \mathbb{Z}[x]$ such that $\deg(f) = n$ and $\mathrm{Gal}(K/\mathbb{Q}) = S_n$. What can you say about the roots?

*Answer.* Since $S_n$ acts transitively on roots of $f$ over $K$, $f$ must be irreducible over $\mathbb{Q}$. The Galois group contains permutations of length $2 \leqslant \ell \leqslant n$, hence $f$ contains irreducible factors of degree $2 \leqslant d \leqslant n$ for different primes. The roots of $f$ must be independent in the sense of additive linear combinations and multiplicative power combinations.

54. How many automorphisms does the complex field have? How can you extend a simple automorphism (e.g. $\sqrt{2} \mapsto -\sqrt{2}$) of an algebraic field into $\mathbb{C}$? How can you extend a general subfield isomorphism? What feature of $\mathbb{C}$ allows you to?

*Answer.* There are only two continuous automorphisms on $\mathbb{C}$ that is compatible with the topology. If we drop the topology, there must be infinitely ($2^{\aleph_0}$-uncountably) many of them.

It is not true that any isomorphism between subfields of $\mathbb{C}$ can be extended to $\mathbb{C}$. See Question 55 below for a counterexample. However, one can always extend it to some subfield that is isomorphic to $\mathbb{C}$. Given an isomorphism $K \to L$ of number fields in $\mathbb{C}$. Then $K \otimes_{\mathbb{Q}} \mathbb{Q}_p \to L \otimes_{\mathbb{Q}} \mathbb{Q}_p$ for some $p$ is naturally constructed, and can be extended to $\overline{\mathbb{Q}_p}$. Indeed, one can fix some $\overline{\mathbb{Q}_p} \cong \mathbb{C}$ to translate this argument onto $\mathbb{C}$.

*Remark.* The feature of $\mathbb{C}$ we have used here is that any algebraic closure of any subfield (especially, local subfield) of $\mathbb{C}$ is contained in $\mathbb{C}$. Hence we can construct isomorphisms to $\mathbb{C}$ such as $\overline{\mathbb{Q}_p} \cong \mathbb{C}$.

55. Can it happen that a proper subfield of $\mathbb{C}$ is isomorphic to $\mathbb{C}$? How?

*Answer.* Yes. Choose a countable set of elements of $\mathbb{C}$ (not necessarily transcendental over $\mathbb{Q}$), say $\{\alpha_n\}_{n\in\mathbb{N}}$. Consider $\sigma \in \mathrm{Aut}(\mathbb{Q}(\alpha_0, \alpha_1, \cdots))$ such that $\sigma(\alpha_i) = \alpha_{i+1}$. Apply Zorn's lemma to

$$\mathfrak{F} = \{\widetilde{\sigma} \text{ extension of } \sigma \text{ to } \mathbb{C} : \alpha_0 \notin \operatorname{im} \widetilde{\sigma}\},$$

and we get a maximal element (in the sense of restriction) $f \in \mathfrak{F}$, whose image is isomorphic to $\mathbb{C}$ such that $\alpha_0 \in \mathbb{C} - f(\mathbb{C})$.

56. Consider the minimal polynomial $f(x)$ for a primitive $m$-th root of unity. Prove that if $p$ divides $f(a)$ for some integer $a$ and $(p, m) = 1$, then $m$ divides $p - 1$. Use this fact to show that there are infinitely many primes congruent to 1 mod $m$.

*Proof.* By assumption $a$ is the image of $\zeta_m$ in $\mathbb{F}_p$. Then $a^m = 1$ from $(p, m) = 1$. Since $\zeta$ is the primitive root, we see $a$ has order $m$. On the other hand, by Fermat's little theorem, since $a \neq 0$, we have $a^{p-1} = 1$, which shows that $m \mid (p - 1)$. By varying the choice of $a$ with $m$ fixed, $f(a)$ can have infinitely many possible prime divisors. Since there are only finitely many $p$ such that $(p, m) = p$, we have infinitely many $p$ such that $m \mid (p - 1)$, namely $p \equiv 1 \bmod m$.

57. What is Dirichlet's theorem about primes in arithmetic progression? What can you say about the density of such primes?

*Statement.* (Dirichlet) Given coprime integers $a, m$, there are infinitely many primes $p$ such that $p \equiv a \bmod m$. Namely, there are infinitely many primes lies in a fixed arithmetic progress.

*Theorem.* (Chebotarev) Let $E/F$ be a Galois (not necessarily finite) extension, then

$$\delta\{p \in \mathcal{O}_F \text{ prime} : p \nmid \operatorname{disc}_{E/F}, \operatorname{Frob}_p \in C\} = \frac{\#C}{\#\operatorname{Gal}(E/F)}.$$

Namely, the density of some unramified primes whose Frobenius maps form a conjugacy class $C$ in $\operatorname{Gal}(E/F)$ equals to the proportion of $C$ in $\operatorname{Gal}(E/F)$.

*Application.* It turns out that $\delta\{p \in \mathbb{Z} \text{ is prime} : p \equiv a \bmod m\} = 1/\varphi(m) \neq 0$, hence these primes are infinitely many: consider the cyclotomic extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ for which

$$G := \operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times.$$

Here we get an abelian cyclic group whose conjugacy classes are given by single elements. Since $(a, m) = 1$, we have

$$\begin{aligned} \mathbb{Z}/\varphi(m)\mathbb{Z} &\longrightarrow \operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \\ a \bmod m &\longmapsto (\zeta_m \mapsto \zeta_m^a). \end{aligned}$$

Hence the conjugacy class $C = \{\operatorname{Frob}_a\}$, and the density is $\#C/\#G = 1/\varphi(m)$.

58. How many irreducible polynomials of degree six are there over $\mathbb{F}_2$?

*Solution.* The splitting field of any irreducible polynomial of degree 6 over $\mathbb{F}_2$ is $\mathbb{F}_{2^6}$. The root system is generated by $\alpha \in \mathbb{F}_{2^6} - (\mathbb{F}_{2^2} \cup \mathbb{F}_{2^3})$. Any Galois action is given by $\operatorname{Frob}_2$ as a permutation on roots. Note that $\mathbb{F}_{2^2} \cap \mathbb{F}_{2^3} = \mathbb{F}_2$ and those irreducible polynomials must be monic over $\mathbb{F}_2$, hence

$$\frac{2^6 - 2^3 - 2^2 + 2}{6} = 9$$

counts the number as desired.

59. Can you have a degree 7 irreducible polynomial over $\mathbb{F}_p$? How about a degree 14 irreducible polynomial?

*Solution.* Over $\mathbb{F}_p$, there are $(p - 1)(p^7 - p)/7$ irreducible polynomials of degree 7, and $(p-1)(p^{14} - p^7 - p^2 + p)/14$ irreducible polynomials of degree 14. For the reason, see Question 58.

60. How many irreducible polynomials are there of degree 4 over $\mathbb{F}_2$?

*Solution.* The number is $(2^4 - 2^2)/4 = 3$. In an explicit description, they must have constant item 1 with odd number of monomials:

$$x^4 + x + 1, \quad x^4 + x^3 + 1, \quad x^4 + x^3 + x^2 + x + 1.$$

Here $x^4 + x^2 + 1 = (x^2 + x + 1)^2$ is not irreducible.

61. For each prime $p$, give a polynomial of degree $p$ that is irreducible over $\mathbb{F}_p$. You can do it in a "uniform" way.

*Construction.* The answer is $x^p - x - 1$. This polynomial, which is irreducible modulo $p$, must be a factor of $x^{p^p} - 1$. It is because an irreducible polynomial of degree $p$ has splitting field $\mathbb{F}_{p^p}/\mathbb{F}_p$, and $x^{p^p} - 1$ runs through all elements of $\mathbb{F}_{p^p}$ as its roots. On the other hand, by Fermat's little theorem, $x^p - x - 1$ has value $-1$ for all $x \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

62. Can we solve general quadratic equations by radicals? And what about cubic and so on? Why can't you solve 5-th degree equations by radicals?

*Proposition.* Over a characteristic 0 field, a polynomial is radically solvable if and only if the Galois group of its splitting field is solvable.

*Answer.* General quartic, cubic, and quadratic equations are all radically solvable. However, neither $A_5$ nor $S_5$ are solvable groups.

63. Talk about solvability by radicals. Why is $S_5$ not solvable? Why is $A_5$ simple?

*Answer.* See Question 62 above. Since $A_5$ is simple and has no normal subgroups, there will never be such an ascending sequence whose subquotients $G_j/G_{j-1}$ are abelian. So $S_5$ is not solvable.

*Proof idea.* To show that $A_5$ is simple, one way is by considering the sizes of its conjugacy classes. Another way is by using a fact that for $n \geqslant 5$, every nontrivial conjugacy class in $A_n$ contains at least $n$ elements (c.f. Set I, Question 21).

64. For which $n$ can a regular $n$-gon be constructed by ruler and compass?

*Answer.* A regular $n$-gon is constructible if and only if $\alpha = \cos(\frac{2\pi}{n})$ is constructible, which is equivalent to $[\mathbb{Q}(\alpha), \mathbb{Q}]$ is a power of 2. It turns out to be $n = 2^k p_1 \cdots p_t$, where $p_i = 2^{2^{n_i}} + 1$ are Fermat primes.

65. How do you use Galois theory (or just field theory) to prove the impossibility of trisecting an angle? Doubling a cube? Squaring a circle?

*Recipe.* Saying "constructible" means the ratio of volumes, the cosine or sine of angles, etc. are all constructible. A number $\alpha$ is said to be constructible if $\alpha$ lies in the top of a finite tower of real quadratic extensions starting from $\mathbb{Q}$.

*Proof.* **Trisecting an angle:** over the number field $K = \mathbb{Q}(\cos\theta)$, the tripled cosine equality $\cos\theta = 4\cos^3(\theta/3) - 3\cos(\theta/3)$ shows that $[K(\cos(\theta/3)) : K] = 3$.

**Doubling a cube:** this requires $\sqrt[3]{2}$ to be constructible; but $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

**Squaring a circle:** this requires $\sqrt{\pi}$ to be constructible, and hence $\pi$ is constructible; but the contradiction lies in that $\pi$ is transcendental over $\mathbb{Q}$.

66. Which numbers are constructible? Give an example of a non-constructible number whose degree is nevertheless a power of 2.

    *Answer.* See Question 65 above.

67. State and prove Eisenstein's Criterion.

    *Statement.* Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$. If there is a prime $p$ such that $p \mid a_{n-1}, \ldots, a_0$ but $p \nmid a_n$, $p^2 \nmid a_0$, then $f$ is irreducible over $\mathbb{Z}$.

    *Proof.* Suppose $f = gh$ in $\mathbb{Z}[x]$. Since $f \equiv a_n x^n \bmod p$ and $\mathbb{F}_p[x]$ is a UFD, we get $g \equiv b_i x^i \bmod p$ and $h \equiv c_j x^j \bmod p$ for $i + j = n$. So the constant terms of $g, h$ over $\mathbb{Z}$ are divisible by $p$, hence $p^2 \mid a_0$, a contradiction.

68. Why is $f(x) = (x^p - 1)/(x - 1)$ irreducible over $\mathbb{Q}$?

    *Proof.* It's because $f(x + 1)$ is Eisenstein at $p$.

69. Can you prove the fundamental theorem of algebra using Galois theory? What do you need from analysis to do so?

    *Galois-theoretic Proof.* We have to show any $f(x) \in \mathbb{R}[x]$ has a root in $\mathbb{C} = \mathbb{R}[i]$. Suppose $f(x) \neq x^2 + 1$ is monic and irreducible. Note that when $2 \nmid \deg f(x)$, there is a real root of $f(x)$. (This is the key feature of $\mathbb{R}$ that depends only on the Mean Value Theorem.) Let $E$ be the splitting field of $(x^2 + 1)f(x)$. But one can show that $E = \mathbb{C}$.

    *Details.* Note that $E \supset \mathbb{C}$ and we aim to show the equality. Since $\mathbb{R}$ has characteristic 0, $(x^2 + 1)f(x)$ is separable, and so $E$ is Galois over $\mathbb{R}$. Since $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}$, there exists a Sylow 2-subgroup of $\mathrm{Gal}(E/\mathbb{R})$, say $H$. Consider $\mathbb{R} \subset M = E^H \subset E$. We obtain $[M : \mathbb{R}] = [G : H]$ by Galois theory. On the other hand, $2 \nmid [G : H]$ by Sylow's theorems. So for each $\alpha \in M$, its minimal polynomial is of an odd degree, and obtains a real root. It forces $\alpha \in \mathbb{R}$, and hence $M = \mathbb{R}$ with $G = H$. It follows that $|\mathrm{Gal}(E/\mathbb{C})| = 2^r$ for some $r \geqslant 0$. If $r > 0$ then $\mathrm{Gal}(E/\mathbb{C})$ has a subgroup $N$ of index 2, and $[E^N : \mathbb{C}] = 2$. So $E^N$ is generated by square roots of elements in $\mathbb{C}$, which is again lying in $\mathbb{C}$. Thus $E^N = \mathbb{C}$ and $r = 0$. We accomplish the proof that $E = \mathbb{C}$.

    *Analytic Proof.* We can use real differential calculus involving the Extreme Value Theorem for real-valued functions of two real variables. Alternatively, let $f : \mathbb{C} \to \mathbb{C}$ be any polynomial, then there exists $z_0 \in \mathbb{C}$ where $|f(z)|$ attains its minimum in $\mathbb{R}$.

70. What are the symmetric polynomials?

    *Answer.* Those are unchanged if their variables are arbitrarily permuted.

71. State the fundamental theorem of symmetric polynomials.

    *Statement.* Any symmetric polynomial can be expressed into a polynomial (over the base field) of elementary symmetric polynomials.

72. Is the discriminant of a polynomial always a polynomial in the coefficients? What does this have to do with symmetric polynomials?

    *Answer.* Yes. The discriminant is a symmetric polynomial in all roots, and hence a polynomial of elementary symmetric ones. But the elementary ones are coefficients. Here we have used the the fundamental theorem of symmetric polynomials.

73. Find a non-symmetric polynomial whose square is symmetric.

    *Solution.* For example, the root of the discriminant.

74. Let $f$ be a degree 4 polynomial with integer coefficients. What's the smallest finite field in which $f$ necessarily has four roots?

    *Solution.* Consider $\overline{f} \in \mathbb{F}_p[x]$. If it is irreducible of degree 4, then $\mathbb{F}_{p^4}$ contains all of its roots. The smallest one (in the sense of size) can be $\mathbb{F}_{16}$.

75. Define $p$-adic numbers. What is a valuation?

    *Definition.* For a fixed prime $p$, the most usual definition is to say $p$-adic number $\mathbb{Q}_p$ is the topological completion of $\mathbb{Q}$ with respect to the non-archimedean absolute value $|\cdot|_p := (1/p)^{\mathrm{ord}_p(\cdot)}$.

    *Remark.* By Ostrowski's theorem, any nontrivial non-archimedean absolute value on $\mathbb{Q}$ is equivalent to (i.e. is some integral power of) the $p$-adic valuation for some prime $p$. Also, any nontrivial archimedean absolute value on $\mathbb{Q}$ is equivalent to $|\cdot|_\infty$.

    *Answer.* A valuation is a surjective homomorphism $v : K^\times \to \mathbb{Z}$ defined over a field $K$. It is often taken as a logarithm of some $|\cdot|$.

76. What's Hilbert's theorem 90?

    *Theorem.* (Hilbert 90) Suppose $G$ is a (Galois) group and $M$ is an abelian group equipped with a $G$-action. Then define the first order **group cohomology** by

$$H^1(G, M) := \frac{\{f : G \to M \text{ such that } f(gh) = f(g)^h f(h) \text{ for all } g, h \in G\}}{\{f : G \to M \text{ such that } f(g) = x(x^g)^{-1} \text{ for some } x \in M\}}.$$

    If $L/K$ be a finite Galois extension with Galois group $G$. Then $H^1(G, L^\times) = 0$.

77. Consider a nonconstant function between two compact Riemann Surfaces. How is it related to Galois theory and algebraic number theory?

    *Answer.* Let $X$ and $Y$ be compact connected Riemann surfaces, and let $\alpha : Y \to X$ be a nonconstant holomorphic mapping. Write $\mathcal{M}(X)$ and $\mathcal{M}(Y)$ for the fields of meromorphic functions on $X$ and $Y$. The map $f \mapsto f \circ \alpha$ is an inclusion $\mathcal{M}(X) \hookrightarrow \mathcal{M}(Y)$ which makes $\mathcal{M}(Y)$ into a field of finite degree over $\mathcal{M}(X)$; let $m$ be this degree. Geometrically, the map is $m$-to-1 except at a finite number of branch points.

    Let $P \in X$ and let $\mathcal{O}_P$ be the set of meromorphic functions on $X$ that are holomorphic at $P$ — it is the discrete valuation ring attached to the discrete valuation $\mathrm{ord}_P$, and its maximal ideal $\mathfrak{p}$ is the set of meromorphic functions on $X$ that are zero at $P$. Let $B$ be the integral closure of $\mathcal{O}_P$ in $\mathcal{M}(Y)$. Let $\alpha^{-1}(P) = \{Q_1, \ldots, Q_g\}$ and let $e_i$ be the number of sheets of $Y$ over $X$ that coincide at $Q_i$. Then $\mathfrak{p}B = \prod \mathfrak{q}_i^{e_i}$, where $\mathfrak{q}_i$ is the prime ideal $\{f \in B \mid f(Q_i) = 0\}$.

## Set IV: Normal Forms

1. What is the connection between the structure theorem for modules over a PID and conjugacy classes in the general linear group over a field?

   *Statement.* (aka fundamental theorem of finitely generated modules over a PID) Let $R$ be a PID. For any finitely generated $R$-module $M$, there exists a sequence of (pricipal) $R$-ideals, say $(d_1) \supset (d_2) \supset \cdots \supset (d_n)$ (or equivalently, $d_1 \mid d_2 \mid \cdots \mid d_n$) such that

   $$M \cong \bigoplus_{i=1}^{n} R/(d_i).$$

   *Comment.* This is a general version of the following. For vector spaces over fields, they are all generated by a set of basis flatly. However, the modules are possibly not flat, but they can be realized as quotients over PIDs.

   *Answer.* Two elements of $\mathrm{GL}_n(F)$ are conjugate if and only if they obtain the same **rational canonical form** over $F$. The proof of this fact essentially relies on the structure theorem of finitely generated modules over a PID.

2. Explain how the structure theorem for finitely-generated modules over a PID applies to a linear operator on a finite dimensional vector space.

   *Answer.* Given $T : V \to V$ as supposed for $V$ over $F$. Let $V^T = V$ set-theoretically. Then $V^T$ is an $F[x]$-module that admits actions by $f(T) : V \to V$ with $f \in F[x]$. By the structure theorem,

   $$V^T = \bigoplus_{i=1}^{m} F[x]/(f_i)$$

   with $m \leqslant \dim V = n$, $f_1 \mid \cdots \mid f_m$ for $f_i \in F[x]$. Using Chinese remainder theorem, we see $f_1 \cdots f_m$ is the characteristic polynomial of $T \in \mathrm{GL}_n(F)$.

3. I give you two matrices over a field. How would you tell if they are conjugate or not? What theorem are you using? State it. How does it apply to this situation? Why is $k[T]$ a PID? If two matrices are conjugate over the algebraic closure of a field, does that mean that they are conjugate over the base field too?

   *Answer.* The first several questions are solved by Question 1 and 2.

   It turns out that $k[T]$ is ED via the norm $N = \deg : k[T]\backslash\{0\} \to \mathbb{N}$ (note: here comes the reason why we don't define $\deg(0)$).

   Yes, since the rational canonical form does not depend on any property of fields.

4. If two real matrices are conjugate in $\mathrm{M}_n(\mathbb{C})$, are they necessarily conjugate in $\mathrm{M}_n(\mathbb{R})$ as well?

   *Answer.* Yes. They have the same rational canonical form whose access depends no condition on the base field.

5. Give the $4 \times 4$ Jordan forms with minimal polynomial $(x-1)(x-2)^2$.

   *Solution.* Let $J_n(\lambda)$ denote the Jordan block for some eigenvalue $\lambda$ of size $n \times n$. Then the form is

   $$\mathrm{diag}\{J_2(2), 1, 1\}, \quad \text{or } \mathrm{diag}\{J_2(2), 2, 1\}.$$

6. Talk about Jordan canonical form. What happens when the field is not algebraically closed?

   *Answer.* Jordan canonical form is a diagonally blocked matrix consisting of $J_{n_i}(\lambda_i)$, where $\lambda_i$ is one of the eigenvalues.

   If the base field is not algebraically closed, the characteristic polynomial may not split completely, i.e., some eigenvalue does not lie in the field. So the matrix is possibly not diagonalizable. The existence of Jordan canonical form requires that the field admits an extension to a field that contains all eigenvalues.

7. What are all the matrices that commute with a given Jordan block?

   *Answer.* This can be proved by induction: only polynomials of this Jordan block itself.

8. How do you determine the number and sizes of the blocks for Jordan canonical form?

   *Answer.* The number of blocks is not less than the number of distinct eigenvalues. The exponent of an eigenvalue in the minimal polynomial is exactly the maximal size of the block for this eigenvalue. The minimal polynomial and the invariant factors helps a lot. But all these methods cannot give an explicit solution without further computation.

9. For any matrix $A$ over the complex numbers, can you solve $B^2 = A$?

   *Answer.* This can be done over any algebraically closed field (or somehow a sufficiently large field that allows the computation for Jordan canonical forms). The recipe is to reduce $A$ into the Jordan canonical form. For each Jordan block, say $J(\lambda)$, and for some analytically nice function, say $f : \mathrm{GL}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$, we obtain

$$f(J) = \begin{pmatrix} f(\lambda) & f'(\lambda) & \frac{1}{2!}f^{(2)}(\lambda) & \cdots & \frac{1}{(n-1)!}f^{(n-1)}(\lambda) \\ & f(\lambda) & f'(\lambda) & \ddots & \frac{1}{(n-2)!}f^{(n-2)}(\lambda) \\ & & \ddots & \ddots & \vdots \\ & & & \ddots & f'(\lambda) \\ & & & & f(\lambda) \end{pmatrix}.$$

10. What is rational canonical form?

    *Answer.* Given any matrix $A$, we can find its invariant factors, say $f_1 \mid \cdots \mid f_n$ such that there product is the characteristic polynomial $\operatorname{char poly}(A)$, and $f_n = m(A)$, the minimal polynomial. The rational canonical form is the diagonal block of companion matrices of these.

11. Describe all the conjugacy classes of $3 \times 3$ matrices with rational entries which satisfy the equation $A^4 - A^3 - A + 1 = 0$. Give a representative in each class.

    *Answer.* By assumption we have $(A-1)^2(A^2+A+1) = 0$. It forces that $\operatorname{char poly}(A) = (x-1)(x^2+x+1)$. So the invariant factors are uniquely determined, and the conjugacy class is unique. Its representative in canonical form is written as

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

12. What $3 \times 3$ matrices over the rationals (up to similarity) satisfy $f(A) = 0$, where $f(x) = (x^2+2)(x-1)^3$? List all possible rational forms.

    *Solution.* By Cayley–Hamilton theorem, $\operatorname{char}\operatorname{poly}(A) \mid f$, and it is of degree 3. Then $\operatorname{char}\operatorname{poly}(A) = (x^2+2)(x-1)$ or $(x-1)^3$ because $(x^2+2)$ is irreducible. The possibilities for invariant factors are

    $$(x^2+2)(x-1) \quad \text{or} \quad x-1, x-1, x-1 \quad \text{or} \quad x-1, (x-1)^2 \quad \text{or} \quad (x-1)^3.$$

    The respective rational canonical forms are in the following:

    $$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -2 \\ 0 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -3 \\ 0 & 1 & 3 \end{pmatrix}.$$

13. What can you say about matrices that satisfy a given polynomial (over an algebraically closed field)? How many of them are there? What about over a finite field? How many such matrices are there then?

    *Answer.* By Cayley–Hamilton theorem that holds over all commutative rings; the minimal polynomial of the matrices are factors of the given polynomial $f$. Yet $f$ has nothing to do with the characteristic polynomial. Over an algebraically closed field, each Jordan normal form can be reached by a conjugation from the original matrix $A$ such that $f(A) = 0$. So there are only finitely many types of Jordan normal forms (whereas there is possibly infinitely many $A$'s satisfying $f(A) = 0$). This number is morally bounded by the number of partitions of $n = \deg f$.

    Over the finite fields, the counting argument is essentially related to the number of conjugacy classes of $\mathrm{GL}_n(\mathbb{F}_q)$, which equals to the number of irreducible representations.

14. What is a nilpotent matrix?

    *Answer.* Some $A$ such that $A^n = 0$ for sufficiently large $n$.

15. When do the powers of a matrix tend to zero?

    *Answer.* Consider this on a sufficiently large field such that we can talk about Jordan canonical forms. It turns out that any eigenvalue $\lambda$ should have norm $N(\lambda) < 1$.

16. If the traces of all powers of a matrix $A$ are 0, what can you say about $A$?

    *Claim.* $A$ is nilpotent over fields of characteristic 0.

    *Proof.* Note that

    $$\forall k \in \mathbb{N}, \quad \operatorname{tr}(A^k) = 0 \quad \Longleftrightarrow \quad \forall k \in \mathbb{N}, \quad F_k := \lambda_1^k + \cdots + \lambda_n^k = 0.$$

    As a symmetric monic polynomial, $\operatorname{char}\operatorname{poly}(A) = (\lambda - \lambda_1)\cdots(\lambda - \lambda_n)$ has non-leading coefficients whose forms are polynomials in $F_k$ by **Newton Identity**. Then $\operatorname{char}\operatorname{poly}(A) = \lambda^N$ and hence $A^N = 0$.

17. When and how can we solve the matrix equation $\exp(A) = B$? Do it over the complex numbers and over the real numbers.

*Proposition.* We have the identity for any matrix over any field: $\det(\exp(A)) = \exp(\mathrm{tr}(A))$.

*Answer.* Due to the identity, we see $\exp : \mathrm{M}_{n\times n}(F) \to \mathrm{GL}_n(F)$ is surjective for $F = \mathbb{C}$, but is not surjective for $F = \mathbb{R}$. When $B$ is a real matrix, it is required to have a positive determinant.

18. Say we can find a matrix $A$ such that $\exp(A) = B$ for $B$ in $\mathrm{SL}_n(\mathbb{R})$. Does $A$ also have to be in $\mathrm{SL}_n(\mathbb{R})$? Can you take $A$ to be in $\mathrm{SL}_n(\mathbb{R})$?

*Answer.* According to the formula in Question 17 above, we see $\det(B) = 1 = \exp(\mathrm{tr}(A))$, and hence $\mathrm{tr}(A) = 0$. But this not necessarily implies that $A \in \mathrm{SL}_n(\mathbb{R})$. But we can choose $A$ to be so, because $\mathrm{SL}_n(\mathbb{R})$ is generated by its Lie algebra $\mathfrak{sl}_n(\mathbb{R})$ via exp, whose elements consists of matrices of trace 0.

19. Is a square matrix always similar to its transpose?

*Answer.* Yes. The same characteristic polynomial deduces the same invariant factors, and hence the same rational canonical form.

20. What are the conjugacy classes of $\mathrm{SL}_2(\mathbb{R})$?

*Solution.* Since $\mathbb{R}$ is not algebraically closed, any characteristic polynomial of degree 2 has the form $x^2 + ax + b$. Note that in $\mathrm{SL}_2(\mathbb{R})$, the constant term of characteristic polynomial is the determinant, which is 1. So there are 3 types of invariant factors: $x^2 + ax + 1$ (when it is irreducible); $x - 1, x - 1$; $x + 1, x + 1$, with the corresponding rational canonical forms:

$$\begin{pmatrix} 0 & -1 \\ 1 & -a \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad a \in \mathbb{R}.$$

Note that the last two cases are lead by $a = \pm 2$ respectively. Also note that there are infinitely many conjugacy classes of $\mathrm{SL}_2(\mathbb{R})$ when $a$ varies.

21. What are the conjugacy classes in $\mathrm{GL}_2(\mathbb{C})$?

*Solution.* Since $\mathbb{C}$ is algebraically closed, any characteristic polynomial of degree 2 splits completely as $(x - a)(x - b)$. The invariant factors are $x - a, x - a$ (with $a = b$) or $x^2 - cx - d$ (with $c = a + b$ and $d = -ab$). Here are the 2 types of conjugacy classes whose rational canonical forms are:

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, \quad \begin{pmatrix} 0 & d \\ 1 & c \end{pmatrix}, \quad a, c, d \in \mathbb{C}.$$

## Set V: Matrices and Linear Algebra

1. What is a bilinear form on a vector space? When are two forms equivalent? What is an orthogonal matrix? What's special about them?

   *Definitions.* A bilinear form is a function $B : V \times V \to K$ that is linear in each argument separately, where $V$ is a $K$-vector space. For bilinear forms $B_1$ and $B_2$ that map the diagonal $(v, v)$ to $v^T B_1 v$ and $v^T B_2 v$ respectively, they are equivalent if their diagonal images are differed by a linear transformation $\sigma$, say $B_1 = \sigma^T B_2 \sigma$. A matrix $X$ is orthogonal if and only if $X^T X = 1$. Namely, the column vectors of an orthogonal matrix form an orthonormal basis.

   *Remark.* Note that over an algebraically closed field, two bilinear forms are equivalent if and only if they share the same rank; the assumption for the field here is necessary. Also note that orthogonality is equivalent to orthonormality for a matrix over any field of characteristic 0.

2. What are the possible images of the unit circle under a linear transformation of $\mathbb{R}^2$?

   *Answer.* If the linear transformation degenerates, then the image can be a point or a line segment. Consider else the action of $\mathrm{GL}_2(\mathbb{R})$. Each element $\sigma$ maps $(x, y)^T$ to $\sigma(x, y)^T$ and then

   $$x^2 + y^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x & y \end{pmatrix} \sigma^T \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} x \\ y \end{pmatrix}.$$

   Here the new quadratic form is defined by a positive-definite matrix $\sigma^T \sigma$, and hence defines an ellipse.

3. Explain geometrically how you diagonalize a real quadratic form.

   *Explanation.* For a real quadratic form $p(x, y) = Ax^2 + 2Bxy + Cy^2$ defined by real symmetric matrix $T$ (which is always diagonalizable), we have two real eigenvalues $\lambda_{1,2}$ such that $\lambda_1 \lambda_2 = \det T = AC - B^2 = -\Delta/4$. Then there are three types from the aspect of affine geometry:

   (1) $\Delta < 0$ and $\det T > 0$: $p$ defines an ellipse.
   (2) $\Delta = 0$ and $\det T = 0$: $p$ defines a parabola.
   (3) $\Delta > 0$ and $\det T < 0$: $p$ defines a hyperbola.

4. Do you know Witt's theorem on real quadratic forms?

   *Statement.* (Witt) Suppose $k$ is a field with $\mathrm{char}(k) \neq 2$. Let $V$ be a finite-dimensional $k$-vector space equipped with a skew-symmetric bilinear form $B : (u, v) \mapsto u^T B v$, i.e., $B^T = -B$. Then for any subspace $W$ of $V$, an arbitrary isometry $f : W \to W$ on $W$ extends to $\tilde{f} : V \to V$. (Recall that an isometry is a bijection that preserves the distance defined by the inner product with respect to $B$.)

5. Classify real division algebras.

   *Answer.* Under the finite-dimensional assumption, it can be either of $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{H}$ (see Question 49 in Set VI).

6. Consider the simple operator on $\mathbb{C}$ given by multiplication by a complex number. It decomposes into a stretch and a rotation. What is the generalization of this to operators on a Hilbert space?

   *Proposition.* Let $A$ be a bounded linear operator between Hilbert spaces, then $A = UP$ for some partial isometry $U$ and non-negative self-adjoint operator $P$. Moreover, the initial space of $U$ is the closure of the range of $P$.

   *Answer.* The desired analogue is the **Polar Decomposition** as follows, dictating that each bounded linear operator between Hilbert spaces can decompose into an isometry (which preserves distance) and a non-negative operator (which scales distances).

7. Do you know about singular value decomposition?

   *Explanation.* The singular value decomposition of an $m \times n$ matrix $M$ over $\mathbb{C}$ is read as $M = U\Sigma V^*$, where $U$ is an $m \times m$ unitary matrix, $V$ is an $n \times n$ unitary matrix, and $\Sigma$ is an $m \times n$ rectangular unitary matrix. More precisely,

   - columns of $V$ are eigenvectors of $M^*M$;
   - columns of $U$ are eigenvectors of $MM^*$;
   - singular values on the diagonal of $\Sigma$ are non-negative square roots of eigenvalues of $MM^*$ and $M^*M$.

   The geometric content of the SVD theorem can thus be summarized as follows: for every linear map $T : \mathbb{C}^n \to \mathbb{C}^m$ one can find orthonormal bases of $\mathbb{C}^n$ and $\mathbb{C}^m$ such that $T$ maps the $i$th basis vector of $\mathbb{C}^n$ to a non-negative multiple of the $i$th basis vector of $\mathbb{C}^m$, and sends the left-over basis vectors to zero. With respect to these bases, the map T is therefore represented by a diagonal matrix with non-negative real diagonal entries.

8. What are the eigenvalues of a symmetric matrix?

   *Answer.* All eigenvalues of a real symmetric (and hence Hermitian) matrix must be real; moreover, a symmetric matrix can always be diagonalized orthogonally. The result for a general symmetric (e.g. yet not necessarily Hermitian) matrix is possibly unclear.

   *Addendum.* All eigenvalues of an $n \times n$ skew-Hermitian matrix (i.e., $A^* = -A$) are either zero or purely imaginary. Furthermore, $\det A$ is purely imaginary or zero when $n$ is odd, and is real when $n$ is even.

   As for a comparison to the real case, recall that a square matrix is Hermitian if and only if it is unitarily diagonalizable with real eigenvalues.

9. What can you say about the eigenvalues of a skew-symmetric matrix?

   *Answer.* See Question 8 above. Every skew-symmetric matrix has either zero or purely imaginary eigenvalues. In particular, real skew-symmetric matrix are Hermitian. To prove this, suppose $Av = \lambda v$ with $v \in \mathbb{C}^n$ and take $(\cdot)^*$ on both sides of $v^*Av = \lambda v^*v$, where $v^*v \in \mathbb{R}$.

10. Prove that the eigenvalues of a Hermitian matrix are real and those of a unitary matrix are unitary.

    *Proof.* For the first part, use the same strategy as in Question 8. The second part means to say for a unitary matrix $U$, there is a unitary $P$ such that $P^*UP = D =$

$\mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ with $|\lambda_i| = 1$. We only do prove for $n = 2$ and the same argument can be used for the induction. Assuming the existence of $P$, it is easy to see

$$D^*D = \begin{pmatrix} \lambda_1^*\lambda_1 & 0 \\ 0 & \lambda_2^*\lambda_2 \end{pmatrix} = (P^*UP)^*(P^*UP) = P^*(U^*(PP^*)U)P = I.$$

As for the existence of $U$, c.f. Question 11 below.

11. Prove that unitary matrices can be diagonalized by unitary matrices.

*Proof.* Suppose the result is true for all unitary matrices of order $n-1$, and consider a unitary matrix $U = U_1$ of order $n$. Let $\lambda_1$ be an eigenvalue of $U$, and let $v_1$ be a unit eigenvector (scaled to have unity norm) associated with $\lambda_1$. Choose $V_1$ such that $P_1 = \begin{pmatrix} v_1 & V_1 \end{pmatrix}$ is a unitary matrix. (Columns of $V_1$ complete $\{v_1\}$ to an orthonormal basis for $\mathbb{C}^{n\times 1}$.) Then $v_1^*V_1 = 0$ and $V_1^*v_1 = 0$ from which we obtain

$$P_1^*U_1P_1 = \begin{pmatrix} v_1^* \\ V_1^* \end{pmatrix} U_1 \begin{pmatrix} v_1 & V_1 \end{pmatrix} = \begin{pmatrix} \lambda_1 v_1^*v_1 & \lambda_1^* v_1^*V_1 \\ \lambda_1 V_1^*v_1 & V_1^*U_1V_1 \end{pmatrix} = \begin{pmatrix} v_1^*U_1v_1 & v_1^*U_1V_1 \\ V_1^*U_1v_1 & V_1^*U_1V_1 \end{pmatrix}$$

Since

$$(P_1^*U_1P_1)^*(P_1^*U_1P_1) = P_1^*U_1^*P_1P_1^*U_1P_1 = I,$$

we have

$$\begin{pmatrix} \lambda_1^*\lambda_1 & 0 \\ 0 & U_2^*U_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & I \end{pmatrix}.$$

which implies that $\lambda_1^*\lambda_1 = 1$, that is, $|\lambda_1|^2 = 1$, and that $U_2$ is unitary. Let $U_2$ have the eigenvalues $\lambda_2, \ldots, \lambda_n$. Then they are also eigenvalues of $U = U_1$. Since $U_2$ is of order $n-1$, by induction hypothesis $|\lambda_2|^2 = \cdots = |\lambda_n|^2 = 1$ and there exists a unitary matrix $P_2$ such that

$$P_2^*U_2P_2 = D_2 = \mathrm{diag}(\lambda_2, \ldots, \lambda_n).$$

Let

$$P = P_1 \begin{pmatrix} 1 & \\ & P_2 \end{pmatrix}.$$

Then

$$\begin{aligned} P^*UP &= \begin{pmatrix} 1 & \\ & P_2^* \end{pmatrix} P_1^*U_1P_1 \begin{pmatrix} 1 & \\ & P_2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & \\ & P_2^* \end{pmatrix} \begin{pmatrix} \lambda_1 & 0 \\ 0 & U_2 \end{pmatrix} \begin{pmatrix} 1 & \\ & P_2 \end{pmatrix} \\ &= \begin{pmatrix} \lambda_1 & 0 \\ 0 & D_2 \end{pmatrix} = D_1. \end{aligned}$$

*Remark.* As a corollary, real symmetric matrices can be diagonalized by orthogonal matrices.

12. To which operators does the spectral theorem for symmetric matrices generalize?

*Answer.* To self-adjoint operators on Hilbert spaces.

(a) (For symmetric matrices) If $A$ is Hermitian, then there exists an orthonormal basis of $V$ consisting of eigenvectors of $A$. Each eigenvalue is real.

(b) (Generalized version) Suppose $A$ is a compact self-adjoint operator on a (real or complex) Hilbert space $V$. Then there is an orthonormal basis of $V$ consisting of eigenvectors of $A$. Each eigenvalue is real.

13. Given a skew-symmetric/skew-Hermitian matrix $S$, show that $U = (I + S)(I - S)^{-1}$ is orthogonal/unitary.

*Proof.* We only work on $\mathbb{C}$ to show the rough idea. Recall that the spectrum of $S$ in contained in $i\mathbb{R}$ as all eigenvalues of a skew-Hermitian matrix are either purely imaginary or zero (see Question 9). Then the spectrum of $I - S$ cannot contain zero, and hence $A = I - S$ is nondegenerate and invertible. Note that $A^* = I + S$ by assumption. On the other hand, $A^*$ and $A$ are commutative as $(I+S)(I-S) = I-S^2$. Then

$$(A^*A^{-1})^*A^*A^{-1} = (A^{-1})^*AA^*A^{-1} = (A^{-1})^*A^*AA^{-1} = (AA^{-1})^*AA^{-1} = I.$$

14. If a linear transformation preserves a nondegenerate alternating form and has $k$ as an eigenvalue, prove that $1/k$ is also an eigenvalue.

*Explanation.* A bilinear form $A$ on a vector space $V$ (over a field $k$) is called an alternating form if for all $v \in V$, $A(v, v) = 0$. The matrix of $A$ essentially have the block form $\operatorname{diag}(r_1S, r_2S, \ldots, r_mS)$, where

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

*Loose Proof.* Without loss of generality we suppose $\dim V = 2$ and $A = S$. Then for such a linear transformation satisfying $P^TSP = S$, one can check this is equivalent to $\det P = 1$. Once $P$ obtains an eigenvalue $k$, the other eigenvalue should be $1/k$.

15. State/prove the Cayley–Hamilton theorem.

*Statement.* (Cayley–Hamilton) Over any field, matrices satisfy the equations given by their characteristic polynomials.

*Proof.* Over an algebraically closed field $K$, use the Zariski topology on $M_n(K) \simeq \mathbb{A}_K^{n^2}$ and follow the recipe below.

(1) Recall that all Zariski open sets are dense by definition.

(2) Denote $f_A$ by the characteristic polynomial of $A$. The set

$$\{A \in M_n(K) : f_A(A) = 0 \text{ for some } f \in K[x]\} = V(I)$$

(for some ideal $I \subset K[x]$) is Zariski closed in $M_n(K)$ and contains all diagonalizable matrices with distinct eigenvalues.

(3) The set for diagonalizable matrices with distinct eigenvalues is defined as

$$\{A \in M_n(K) : \operatorname{disc} f_A \neq 0\},$$

which is Zariski open, and hence dense.

(4) Consequently, any closed set containing an open dense subset would also be the whole space.

16. Are diagonalizable $N \times N$ matrices over the complex numbers dense in the space of all $N \times N$ matrices over the complex numbers? How about over another algebraically closed field if we use the Zariski topology?

    *Answer.* Yes. See Question 15 above. For general fields, use the same argument, by base extension of the field to its algebraic closure and using the fact that diagonalizable matrices are Zariski dense in the space of all matrices.

17. For a linear ODE with constant coefficients, how would you solve it using linear algebra?

    *Answer.* Formally, we obtain the solution of the initial value problem $X' = AX$ with initial data $X(t_0) = (c_1, c_2)^T$ as

    $$e^{A(t-t_0)}X(t_0),$$

    where for a given matrix $A$, the exponential $e^A$ is defined as

    $$e^A = I + A + \frac{A^2}{2} + \cdots + \frac{A^n}{n!} + \cdots.$$

    Explicitly, take the case $n = 2$ for example. For $X' = AX$ we suppose $\lambda_{1,2}$ are eigenvalues of $A$ and $v_{1,2}$ are corresponding eigenvectors (not necessarily real).

    - When $\lambda_{1,2}$ are real and $A$ is diagonalizable,

      $$X(t) = c_1 e^{\lambda_1 t} v_1 + c_2 e^{\lambda_2 t} v_2.$$

    - When $\lambda_1 = \lambda_2 = \lambda$ and $A$ is not diagonalizable,

      $$X(t) = c_1 e^{\lambda t} v_1 + c_2 (t e^{\lambda t} v_1 + e^{\lambda t} v_2),$$

      where $(A - \lambda I)v_1 = (A - \lambda I)^2 v_2 = 0$, $(A - \lambda I)v_2 = v_1$.

    - When $\lambda_{1,2} = \alpha \pm i\beta$ with $v_{1,2} = u \pm iw$,

      $$X(t) = c_1 e^{\alpha t}((\cos \beta t)u - (\sin \beta t)w) + c_2 e^{\alpha t}((\sin \beta t)u + (\cos \beta t)w).$$

18. What can you say about the eigenspaces of two matrices that commute with each other?

    *Answer.* For two matrices that commute mutually, one fixes all eigenspaces of another. If they happen to be diagonalizable, they can be diagonalized by the same matrix simultaneously.

19. What is a Toeplitz operator?

    *Answer.* A Toeplitz operator acting on the Hilbert space $L^2$ is defined by a two-sided complex sequence $(a_n)_{n=-\infty}^{\infty}$. It can be realized as a diagonal-constant matrix looking like

    $$T = \begin{pmatrix} a_0 & a_{-1} & a_{-2} & \cdots \\ a_1 & a_0 & a_{-1} & \ddots \\ a_2 & a_1 & a_0 & \ddots \\ \vdots & \ddots & \ddots & \ddots \end{pmatrix}.$$

    *Punchline.* Recall that the spectrum of $T$ is $\{\lambda \in \mathbb{C} : \det(T - \lambda I) = 0\}$. Then every Toeplitz operator has connected spectrum, and those $T - \lambda I$ are not invertible modulo the compact operators.

20. What is the number of invertible matrices over $\mathbb{Z}/p\mathbb{Z}$?

*Solution.* Consider a matrix in $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ from the first column. It has $p^n-1$ nonzero choices, and the 2nd column has $p^n-p$ choices because it is linearly independent from the first choice. Do this in iteration to get

$$|\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})| = \prod_{i=0}^{n-1}(p^n - p^i).$$

## Set VI: Rings

1. State the Chinese remainder theorem in any form you like. Prove it.

   *Statement.* Given any two ideals $I, J$ of $R$ such that $I + J = (1)$, then

   $$\begin{aligned} R/(I \cap J) &\longrightarrow R/I \times R/J \\ x \bmod (I \cap J) &\longmapsto (x \bmod I, x \bmod J) \end{aligned}$$

   is an isomorphism. This can be generalized inductively to countably many ideals who are mutually coprime.

   *Classical Statement.* For an integer $n = p_1^{e_1} \cdots p_k^{e_k}$, we obtain

   $$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{e_k}\mathbb{Z}.$$

   *Proof.* The coprime condition is essential to deduce

   $$(I + J)/(I \cap J) \cong (I + J)/I \times I/(I \cap J) \cong (I + J)/I \times (I + J)/J.$$

   So $R/(I \cap J) \cong R/I \times R/J$. Here we have used the 2nd isomorphism theorem.

2. What is a PID? What's an example of a UFD that is not a PID? Why? Is $k[x]$ a PID? Why?

   *Answer.* A PID is an integral domain in which every ideal is principal. The ring $k[x]$ is a ED via the degree function.

   *Example.* See Question 3.

   *Fact.* All polynomial rings over a UFD, all formal power series rings over a field, and all regular local rings are all UFDs.

3. Is $\mathbb{C}[x, y]$ a PID? Is $\langle x, y\rangle$ a prime ideal in it?

   *Answer.* $\mathbb{C}[x, y]$ is UFD but not PID, because $\langle x, y\rangle$ is not principal. It is a (even maximal) prime ideal since $\mathbb{C}[x, y]/\langle x, y\rangle \cong \mathbb{C}$ is a field.

4. Do polynomials in several variables form a PID?

   *Answer.* The ring $k[x_1, \ldots, x_n]$ is not a PID (see Question 2 and 3) unless $n = 1$.

5. Prove that the integers form a PID.

   *Proof.* Note that $\mathbb{Z}$ is Euclidean via $|\cdot| : \mathbb{Z}\backslash\{0\} \to \mathbb{N}$. Then use Question 7.

   *Remark.* The ring of integers $\mathcal{O}_K$ of any given number field $K$ is a PID if and only if $\mathrm{Cl}(K) = \{1\}$, or equivalently $h(K) = 1$.

6. Give an example of a PID with a unique prime ideal.

   *Answer.* Note that in a PID, all prime ideals are maximal. So a local PID fits this condition.

7. What is the relation between Euclidean domains and PIDs?

   *Answer.* Being Euclidean implies being a PID. Given the value function on ED, any ideal in it is generated by the element with the smallest value.

8. Do you know a PID that's not Euclidean?

   *Upshot.* The tool to check whether a given ring is Euclidean or not: if $R$ is Euclidean, then there is $a \notin R^\times$ such that $R/(a)$ is represented by $\{0\} \cup R^\times$.

   *Answer.* Two examples: $R = \mathbb{Z}[(1+\sqrt{-19})/2]$ or $R = \mathbb{R}[x,y]/(x^2+y^2+1)$.

   To check the former, note that the Minkowski bound $M_{\mathbb{Q}(\sqrt{-19})} < 1$ so $R = \mathcal{O}_{\mathbb{Q}(\sqrt{-19})}$ is a PID. By Dirichlet's unit theorem, $r_1 + r_2 - 1 = 0$ so $R^\times = \mu(R) = \{\pm 1\}$ (this can be attained by norm as well). If there were such $a$, $R/(a)$ would have at most 3 elements with $a \notin R^\times$, so $a \in \{\pm 2, \pm 3\}$. Since $R$ is free of rank 2 over $\mathbb{Z}$, $R/(a) \cong (\mathbb{Z}/2\mathbb{Z})^2$ or $(\mathbb{Z}/3\mathbb{Z})^2$, in which there are respective 4 and 9 elements. Here comes a contradiction.

9. Give an example of a UFD which is not a Euclidean domain.

   *Answer.* Question 8 gives PID that is not ED. Question 3 gives UFD that is not PID.

10. Is a ring of formal power series a UFD?

    *Answer.* A ring of formal power series over a field must be a UFD. But this fails possibly if it is over another UFD.

    *Example.* If $R$ is the localization of $k[x,y,z]/(x^2+y^3+z^7)$ at the prime ideal $(x,y,z)$ then $R$ is a local ring that is a UFD, but $R[\![x]\!]$ is not a UFD.

11. Is a polynomial ring over a UFD again a UFD?

    *Answer.* Yes. Let $R$ be a UFD. Then the factorizations in $R[x]$ realizes as factorizations in $(\mathrm{Frac}(R))[x]$, which is an ED. Applying the one-variable-result for countably many times will deduce the result.

12. What does factorization over $\mathbb{Q}[x]$ say about factorization over $\mathbb{Z}[x]$?

    *Answer.* Since $\mathbb{Q}[x]$ is an ED and hence a UFD containing $\mathbb{Z}[x]$, all elements in $\mathbb{Z}[x]$ factors uniquely in $\mathbb{Q}[x]$. In fact, it is factored into $\mathbb{Z}[x]$.

    *Remark.* This is an example of Question 11.

13. Give an example of a ring where unique factorization fails.

    *Example.* See Question 14 for $\mathbb{Z}[\sqrt{-5}]$.

14. Factor 6 in two different ways in $\mathbb{Z}[\sqrt{-5}]$. Is there any way to explain the two factorizations? Factor the ideal generated by 6 into prime ideals.

    *Answer.* We have $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$. A possible explanation is $\mathrm{Cl}(\mathbb{Q}(\sqrt{-5})) = \mathbb{Z}/2\mathbb{Z}$ is nontrivial. But at the level of ideals, $(6) = (1+\sqrt{-5})(1-\sqrt{-5})$ where $(1 \pm \sqrt{-5})$ are prime ideals.

    *Note.* At the level of ideals, the uniqueness for factorization is recovered.

15. What's the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(i)$?

    *Answer.* It is $\mathbb{Z}[i]$ since $d = -1 \equiv 3 \bmod 4$.

16. Find all primes in the ring of Gaussian integers.

    *Solution.* Consider how primes in $\mathbb{Z}$ factors in $\mathbb{Z}[i]$ via the extension $\mathbb{Q}(i)/\mathbb{Q}$. Let $p \in \mathbb{Z}$ be a prime. Recall that an odd prime $p = a^2 + b^2$ for $a, b \in \mathbb{Z}$ if and only if $p \equiv 1 \bmod 4$. Given any Gaussian prime $\mathfrak{p}$, note that $\varepsilon\mathfrak{p}$ is another Gaussian prime, where $\varepsilon \in \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

- $p = 2$: since $\operatorname{disc}(x^2+1) = 2^2 = \operatorname{disc}\mathbb{Q}(i)$, the prime $2 \in \mathbb{Z}$ ramifies (yet does not split completely) as $(2) = \mathfrak{p}\mathfrak{p}' = (1+i)(1-i) = i(1-i)^2$. Then $\varepsilon(1-i) \in \mathbb{Z}[i]$ are primes.
- $p \equiv 1 \bmod 4$: now $p = a^2 + b^2 = (a+bi)(a-bi)$ splits completely. Here comes $\varepsilon(a+bi) \in \mathbb{Z}[i]$ such that $a^2 + b^2 = p$.
- $p \equiv 3 \bmod 4$: $p$ keeps inert and this deduces $\varepsilon p \in \mathbb{Z}[i]$ as primes.

17. What is a ring of integers? What does "integral over $\mathbb{Z}$" mean?

*Answer.* It is the ring formed by elements in a fixed number field that are integral over $\mathbb{Z}$. Say an element is integral over $\mathbb{Z}$ if it is a root of some $\mathbb{Z}$-coefficient polynomial.

18. Let $\mathcal{O}$ be the ring of integers of $\mathbb{Q}(\sqrt{d})$, where $d > 0$. What can you say about the quotient of $\mathcal{O}$ by one of its prime ideals?

*Answer.* From algebraic number theory, we know

$$\mathcal{O} = \begin{cases} \mathbb{Z}[\sqrt{d}], & d \not\equiv 1 \bmod 4; \\ \mathbb{Z}[(1+\sqrt{d})/2], & d \equiv 1 \bmod 4. \end{cases}$$

Let $\mathfrak{p}$ be a prime in $\mathcal{O}$ with $\mathfrak{p}\mathcal{O} \cap \mathbb{Z} = p\mathbb{Z}$. Then $p = N(\mathfrak{p}) = |\mathcal{O}/\mathfrak{p}\mathcal{O}|$ and the inertia degree $f(\mathfrak{p}|p) = [\mathcal{O}/\mathfrak{p}\mathcal{O} : \mathbb{Z}/p\mathbb{Z}] \leqslant 2$.

19. Do you know about Dedekind domains and class numbers?

*Definition.* An integral domain is said to be a Dedekind domain if it is noetherian, integrally closed, and every prime ideal in it is maximal (namely, of Krull dimension 1). It turns out that $\mathcal{O}_K$ for a number field $K$ is a Dedekind domain.

*Definition.* The class number $h(K)$ of $K$ is the order of the class group, say $\mathrm{Cl}(K)$, which is the quotient by the group of fractional ideals by an equivalent relation. Two fractional ideals are equivalent if and only if they are differed by some scalar in $K^\times$.

*Remark.* For the scheme $X = \operatorname{Spec}(A)$ with $A$ Dedekind, the class group

$$\mathrm{Cl}(X) := \mathrm{Div}(X)/\sim$$

of Weil divisors on $X$ is the same as the class group of $A$. And $\mathrm{Div}(X)$ is the same as the group of fractional ideals.

*Caution.* Recall that if $R$ is a UFD, so also is $R[x]$. Yet if $R$ is a Dedekind domain, the similar property fails for $R[x]$. To see this, recall that a Dedekind domain locally looks like a discrete valuation ring.

20. Talk about factorization and primes in a polynomial ring. What is irreducibility? For what rings $R$ is it true that $R[x_1, \ldots, x_n]$ is a unique factorization domain? What is wrong with unique factorization if we don't have an integral domain? Now, PIDs are Noetherian, but are there UFDs which are not?

*Definition.* An element $r$ in a ring $R$ is called irreducible if $r = xy$ implies that $x \in R^\times$ or $y \in R^\times$, i.e., any nontrivial factorization involves a unit factor.

*Answer.* If $R$ is a UFD, then $R[x]$ is a UFD. (Yet the converse fails to be true; see some ring of integers of a Hilbert class field versus the ring of integers of its subfield with nontrivial class group.)

All UFDs must be integral. For counterexample, say $R = \mathbb{Z}/6\mathbb{Z}$ in which $6 = 2 \cdot 3 = 2^m \cdot 3^n$ with $m, n \geqslant 1$.

As $R[x_1, \ldots, x_n]$ is a UFD, by induction, $R[x_1, \ldots, x_n, \ldots]$ with infinitely many variables is still a UFD. It is apparently not noetherian because the ascending chain $(x_1) \subset (x_1, x_2) \subset \cdots$ never terminates.

21. What is the radical of an ideal? What is special about elements in the nilradical?

*Definition.* The radical of an ideal $\mathrm{Rad}(I)$ comprises all $n$-th roots of elements in $I$ for all $n \geqslant 1$. It turns out to be the intersection of all prime ideals containing $I$.

*Answer.* The nilradical (resp. Jacobson radical) is the intersection of *all* prime (resp. maximal) ideals in a given ring. Thus,

$$\mathrm{nil}(R) = \mathrm{Rad}(R) \subset \mathrm{Rad}(I), \quad \forall I \subset R.$$

22. Define "radical". Prove it is an ideal. Prove that the ideal of all polynomials vanishing on the zero set of $J$ is $\mathrm{rad}(J)$.

*Definition.* Say $\mathrm{Rad}(I) = \{x \in R : x^n \in I \text{ for some } n \geqslant 1\}$ for $I \subset R$ a given ideal.

*Proof.* The $\mathrm{Rad}(I)$ is an ideal because it's the intersection of all prime ideals containing $I$. By Hilbert's Nullstellensatz, $I(V(J)) = \mathrm{Rad}(J)$ for an ideal $J \subset k[X]$, where $X = \{x_1, \ldots, x_m\}$.

23. Do you know what the radical is? Use the fact that the intersection of all prime ideals is the set of all nilpotent elements to prove that $F[x]$ has an infinite number of prime ideals, where $F$ is a field.

*Answer.* See Question 22 above.

*Proof.* Note that $F[x]$ has no nilpotent element except $0 \in F$: if there is some nilpotent $f$, its degree in $x$ must be 0; but in a field, $a^n = 0$ means $a = 0$. Therefore, $\mathrm{nil}(F[x]) = (0) = \bigcap \mathfrak{p}$ can be an infinite intersection.

*Remark.* This argument is not sufficient here. It seems that something goes wrong.

24. What are the radical ideals in $\mathbb{Z}$?

*Solution.* If $m = p_1^{e_1} \cdots p_k^{e_k} \in \mathbb{Z}$, then $m\mathbb{Z} \subset p_i\mathbb{Z}$ for all $p_i$. Hence

$$\mathrm{Rad}(m\mathbb{Z}) = \bigcap_{i=1}^{k} p_i\mathbb{Z} = p_1 \cdots p_k\mathbb{Z}.$$

So the radical ideals in $\mathbb{Z}$ are given by $m\mathbb{Z}$ for all square-free integers $m$.

25. Give a prime ideal in $k[x, y]$. Why is it prime? What is the variety it defines? What is the Nullstellensatz? Can you make some maximal ideals?

*Answer.* It's $(f(x, y))$, where $f$ is an irreducible polynomial. It is prime because it defines a generic point (not necessarily closed) on $\mathbb{A}_k^2 \cong \mathrm{Spec}\, k[x, y]$. A prime ideal always corresponds to a (topologically) irreducible affine variety. A maximal ideal is in the form $(x - a, y - b)$, which is a closed point of $\mathbb{A}_k^2$. For the Nullstellensatz, see Question 26 below.

26. State/describe Hilbert's Nullstellensatz.

*Statement.* (Nullstellensatz) Let $k$ be any field and $\overline{k}$ be its algebraic closure. Consider the polynomial ring $\overline{k}[X_1, \ldots, X_n]$ in $n$ variables. For any ideal $J \subset \overline{k}[X_1, \ldots, X_n]$ and any open subset $U \subset \mathbb{A}^n_{\overline{k}} = \overline{k}^n$, define that

$$I(U) := \{f \in \overline{k}[X_1, \ldots, X_n] : f(v) = 0 \text{ for all } v \in \overline{k}^n\},$$
$$V(J) := \{v \in \overline{k}^n : f(v) = 0 \text{ for all } f \in J\}.$$

Then $I(V(J)) = \sqrt{J}$.

27. What is an irreducible variety? Give an example of a non-irreducible one.

*Definition.* The variety that cannot expressed as the union of two closed proper subvarieties set-theoretically.

*Example.* A union of two affine lines that intersect transversally, say $\operatorname{Spec} k[x, y]/(xy) = \operatorname{Spec} k[x, y]/(x) \cup \operatorname{Spec} k[x, y]/(y)$.

28. What are the prime ideals and maximal ideals of $\mathbb{Z}[x]$?

*Solution.* Let $\mathfrak{p}$ be a prime in $\mathbb{Z}[x]$. Then $\mathfrak{p} \cap \mathbb{Z} = (0)$ or $(p)$. If it is $(0)$, then $\mathfrak{p} = (f(x))$ for irreducible $f \in \mathbb{Z}[x] \backslash \mathbb{Z}$ or $\mathfrak{p} = (0)$. Otherwise $\mathfrak{p} = (p)$ or $(p, f(x))$ for irreducible $f$. Hence the maximal ideals are $\mathfrak{m} = (p, f(x))$.

*Remark.* This is asking about the classification of points in $\operatorname{Spec} \mathbb{Z}[x]$. The generic point is $(0)$ as usual.

29. Is the map $\mathbb{Z}[t]/(t^p - 1) \to \mathbb{Z}[w]$ given by $t \mapsto w$ where $w^p = 1$ an isomorphism?

*Answer.* Yes (even if there are many choices of $w$). Just consider the natural surjection $\mathbb{Z}[t] \to \mathbb{Z}[w]$ and its kernel.

*Comment.* Yet the map $\mathbb{Z}[t]/(t^p - 2) \to \mathbb{Z}[w]$ given by $t \mapsto w$ where $w^p = 2$ is not an isomorphism. The "cyclic condition for automorphisms" is necessary.

30. Describe the left, right, and two-sided ideals in the ring of square matrices of a fixed size. Now identify the matrix algebra $\mathrm{M}_n(K)$ with $\mathrm{End}_K(V)$ where $V$ is an $n$-dimensional $K$-vector space. Try to geometrically describe the simple left ideals and also the simple right ideals via that identification.

*Discussion.* In $\mathrm{M}_n(R)$ over commutative ring $R$ with unit, there is a bijection between the two-sided ideals of $\mathrm{M}_n(R)$ and the two-sided ideals of $R$. However, not every left or right ideal of $\mathrm{M}_n(R)$ arises by this construction from a left or right ideal in $R$. For example, consider the set of matrices $(a_{ij})$ such that $a_{ij} = 0$ for $2 \leqslant j \leqslant n$. This forms a left ideal but not a right ideal.

*Geometric Description.* When we view $\mathrm{M}_n(K)$ as the ring of linear endomorphisms of $K^n$, those matrices which vanish on a given subspace $W$ of $V$ form a left ideal

$$I(W) := \{X \in \mathrm{M}_n(K) : \forall w \in W,\ Xw = 0\}.$$

Conversely, for a given left ideal $I$ of $\mathrm{M}_n(K)$, the intersection of null spaces of all matrices in $I$ gives a subspace

$$Z(I) := \bigcap_{X \in I} \mathrm{Null}(X)$$

of $K^n$. Under this construction, the left ideals of $\mathrm{M}_n(K)$ are in bijection with the subspaces of $V = K^n$. The case is the same for right ideals.

*Remark.* There is no explicit definition for an ideal to be simple. The second question possibly meant to say a radical (left/right) ideal, to compatible with some theory like Hilbert's Nullstellensatz.

31. Give examples of maximal ideals in $K = \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \cdots$, the product of countably many copies of $\mathbb{R}$. What about for a product of countably many copies of an arbitrary commutative ring $R$?

    *Example.* It can be $\{0\} \times \mathbb{R} \times \mathbb{R} \times \cdots$ (whose residue field in $K$ is exactly $\mathbb{R}$); alternatively, take the maximal ideal that includes the ideal which contains sequences with almost all (namely, all but finitely many) 0's. When I replace $\mathbb{R}$ by $R$, it may not be maximal since the residue is not necessarily a field.

32. Consider a commutative ring, $R$, and a maximal ideal, $I$, what can you say about the structure of $R/I$? What if $I$ were prime?

    *Answer.* $R/I$ is a field if and only if $I$ is maximal. $R/I$ is an integral domain if and only if $I$ is prime.

33. Define "Noetherian ring". Give an example.

    *Definition.* A commutative ring $R$ is called noetherian if each ideal of $R$ is finitely generated. Equivalently, say each infinite increasing ideal sequence eventually stabilizes.

    *Recipe.* To construct a noetherian ring, we use the fact: if $R$ is noetherian, then $R/I$ is noetherian for all ideals $I \subset R$. Hilbert basis theorem must be useful as well.

    *Example.* $\mathbb{Z}[\sqrt{d}]$ is noetherian since it is $\mathbb{Z}[x]/(x^2 - d)$; for any field $K$ (which is trivially noetherian), $K[x, 1/x] \cong K[x, y]/(xy - 1)$ is noetherian as well.

    *Non-Example.* The ring $K[\![x_1, x_2, \ldots]\!]$ of formal power series in infinitely many variables is not noetherian. But the non-noetherian rings need not be really huge: $\mathrm{Int}(\mathbb{Z}) = \{f \in \mathbb{Q}[x] : f(\mathbb{Z}) \subset \mathbb{Z}\}$, the ring of polynomials with integer outputs, is not noetherian.

34. Prove the Hilbert basis theorem.

    *Statement.* If $R$ is a noetherian ring, then so is $R[x]$.

    *Proof Idea.* Choose the element of the minimal degree in a given ideal $(0) \neq I \subset R[x]$, say $f_1$, and consider $I - (f_1)$. Do this iteratively to get $I - (f_1, \ldots, f_k)$ for $k \gg 0$. Then we get a series of generators with minimal degrees. Note that their leading coefficients form a finitely generated ideal in $R$. Hence $x^n(f_1, \ldots, f_k)$ gives polynomials in higher degrees, and $I$ is finitely generated.

35. If $I$ is an ideal in a Noetherian ring with a unit, what is the intersection of $I^n$ over all positive integers $n$?

    *Lemma.* (Krull's Intersection Theorem) Suppose $R$ is a Noetherian domain, then for a fixed proper ideal $I \subset R$ and any finite $R$-module $M$,

    $$\bigcap_{n \geqslant 1} I^n M = 0.$$

*Comment.* This question is in general nontrivial but one can have a relatively easy attempt by assuming $R$ is a Noetherian domain, and then use the Krull's intersection theorem. Note that the assumption for "domain" is necessary to make the intersection to vanish. Say, for a boring counterexample, let $R = S \oplus S$ and $I = S \oplus \{0\}$ where $S$ is noetherian.

36. What is the Jacobson radical? If $R$ is a finitely-generated algebra over a field $k$, what can you say about it?

*Lemma.* A finitely-generated algebra over a field is an integral domain if and only if it is a field. Applying this to $R/I$, we see: An ideal $I \subset R$ is prime if and only if it is maximal.

*Answer.* By definition, the Jacobson radical of $R$ is the intersection of all maximal ideals in $R$. By assumption,

$$\bigcap_{\mathfrak{m} \text{ maximal}} \mathfrak{m} = \bigcap_{\mathfrak{p} \text{ prime}} \mathfrak{p} = \operatorname{nil}(R).$$

37. Give an example of an Artinian ring.

*Definition.* A ring satisfies the descending chain condition on ideals is called Artinian.

*Example.* Let $k$ be an integral domain, then it is Artinian if and only if it is a field. Suppose $k$ is a field, then $k[x]/(x^n)$ is Artinian with maximal ideal $(x)$, and $k[x,y]/(x^2, y^3, xy^2) \cong k[x, y, xy, y^2]$ is Artinian with maximal ideal $(x, y)$.

38. State the structure theorem for semisimple Artinian rings.

*Statement.* (aka Wedderburn–Artin theorem) Given an semisimple Artinian ring $A$, there are integers $n_1, \dots, n_r$ with division rings $D_1, \dots, D_r$ that are uniquely determined by $A$, such that

$$A \cong \bigoplus_{i=1}^{r} \mathrm{M}_{n_i}(D_i).$$

*Alternative Statement.* Any simple Artinian ring can be realized as a matrix ring over some division ring. From this point of view, note that the direct sum can be infinite.

*Punchline.* Recall Maschke's theorem (Question 2 in Set VIII): If $\operatorname{char} k \nmid |G|$ for a field $k$, then the group algebra $k[G]$ is semisimple.

Applying Wedderburn–Artin to the ring (also the vector space) $k[G]$, it factors as direct sum of matrix rings. This means a representation of $G$ decomposes into the irreducibles, and all subrepresentations have orthogonal complements.

39. What is a semisimple algebra? State the structure theorem for semisimple algebras.

*Definition.* A (finite-dimensional) algebra (as a vector space) is said to be semisimple if its nilradical (as a ring) is trivial.

*Statement.* (c.f. Question 38) Let $A$ be a semisimple algebra over a field (not necessarily finite-dimensional). Then

$$A \cong \bigoplus_{i \in I} \mathrm{M}_{n_i}(D_i)$$

for division algebras $D_i$. Conversely, any algebra admitting this decomposition must be semisimple.

*Remark.* A useful fact for computation: the unique division algebra over an algebraically closed field $F$ is $D = F$ itself. Hence the group algebra

$$\mathbb{C}[G] \cong \bigoplus_{i \in I} \mathrm{M}_{n_i}(\mathbb{C}).$$

40. What is a matrix algebra?

*Answer.* The $n \times n$-matrix ring $\mathrm{M}_n(k)$ over $k$ under matrix addition and multiplication is a $k$-algebra. This is called a matrix algebra over $k$.

41. Does $L^1$ have a natural multiplication with which it becomes an algebra?

*Answer.* By definition $L^1$ consists of absolutely Lebesgue-integrable functions. It is a Banach space. Over $\mathbb{C}$, the $L^1$ space becomes a commutative $C^*$-algebra with pointwise multiplication $(f \cdot g)(x) = f(x) \cdot g(x)$ and conjugation. (Recall that a $C^*$-algebra is a Banach algebra together with an involution satisfying the properties of the adjoint, i.e. a $\mathbb{C}$-algebra of continuous linear operators on a complex Hilbert space closed under adjoints and topologically closed in the norm topology of operators.)

42. Consider a translation-invariant subspace of $L^1$. What can you say about its relation to $L^2$ as a convolution algebra?

*Answer.* A translation-invariant subspace of $L^1$ is a closed subspace $V$ of $L^1$ such that for any $f \in V$, the translated function $f(x - y) \in V$. If $V$ is a translation-invariant subspace of $L^1$, then it is also a convolution algebra with $L^2$. Considering that $f * g$ is well-defined when $f \in L^1$ and $g \in L^2$, the translation-invariance of $V$ ensures that $f * g \in V$.

43. State the structure theorem for simple rings.

*Statement.* (Wedderburn) Every simple ring with a unit (and a minimal left ideal) is isomorphic to $\mathrm{M}_{n \times n}(D)$, where $D$ is a division ring. See Question 38.

44. Do you know an example of a local ring? Another one? What about completions?

*Examples.* Any field or valuation ring is local. The stalk $\mathcal{O}_{X,x}$ at some point of an algebraic variety is local. The ring of formal power series $R[\![X_1, \ldots, X_n]\!]$ over any field or any local ring $R$ is local.

The ring $R[\![X_1, \ldots, X_n]\!]$ is already complete whenever $R = k$ is a field. (This is a result of Cohen's Structure Theorem that, over an extension of $k$, a complete regular local ring of Krull dimension $n$ containing $k$ must be a power series ring in $n$ variables.)

45. Consider the space of functions from the natural numbers to $\mathbb{C}$ endowed with the usual law of addition and the following analogue of the convolution product:

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$$

Show that this is a ring. What does this ring remind you of and what can you say about it?

46. Is finite division ring necessarily commutative? Give an example of a (necessarily infinite) division ring which is NOT a field.

*Answer.* Yes. This is the result proved by Wedderburn. Moreover, we see every finite division ring is a field (and hence isomorphic to some $\mathbb{F}_q$ with $q = p^r$).

*Example.* The classical Hamiltonian quaternion does so. In this division ring, the vectors with basis $1, i, j, k$ are divisible by other vectors whereas the commutativity fails to be valid.

47. Prove that all finite integral domains are fields.

*Proof.* The multiplication map on $R$ defined by a nonzero and nonunit element $r \in R - R^\times$ is injective because $R$ is integral. On the other hand, the finiteness assumption deduces that this must be surjective due to the cardinality comparison. Hence the division map is well-defined and then $R$ is a field.

48. Can a polynomial over a division ring have more roots than its degree?

*Answer.* Yes. For example, there are 6 distinct 4th roots of unity in the quaternions

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

See Question 27 of Set I for details.

49. Classify (finite-dimensional) division algebras over $\mathbb{R}$.

*Theorem.* (Frobenius) Let $D$ be a real division algebra whose all elements are algebraic. Then up to isomorphisms, $D$ is isomorphic to $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{H}$ (the quaternion algebra).

*Conclusion.* (Note that all elements in any finite-dimensional algebra are automatically algebraic.) There are three classes $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{H}$ say. If we drop the multiplicative associativity, it can also be the bi-quaternion algebra, denoted by $\mathbb{O}$.

50. Give an example of a $\mathbb{C}$-algebra which is not semisimple.

*Example.* Note that the semisimple algebras have trivial Jacobson radicals (see Question 36 of Set IV for the definition). Consider a finite dimensional $\mathbb{C}$-vector space $V$. And define a $\mathbb{C}$-algebra by

$$R := \left\{ \begin{pmatrix} a & v \\ 0 & b \end{pmatrix} : a, b \in \mathbb{C}, v \in V \right\}.$$

Then $R$ is a $\mathbb{C}$-algebra with $\dim_{\mathbb{C}} R = \dim_{\mathbb{C}} V + 2 < \infty$. However, one can compute

$$\mathrm{nil}(R) = \begin{pmatrix} 0 & V \\ 0 & 0 \end{pmatrix} \neq 0,$$

which dictates the non-semisimplicity of $R$.

51. What is Artin–Wedderburn's theorem? What does the group ring generated by $\mathbb{Z}/5\mathbb{Z}$ over $\mathbb{Q}$ look like? What if we take the noncyclic group of order 4 instead of $\mathbb{Z}/5\mathbb{Z}$? The quaternion group instead of $\mathbb{Z}/5\mathbb{Z}$?

*Statement.* See Question 38 for Artin–Wedderburn.

*Answer.*

52. Tell me about group rings. What do you know about them?

*Answer.* Given a ring $R$ and a multiplicative group $G$, define the group ring

$$R[G] := \{f : G \to R \text{ with finite support}\}.$$

The addition on this ring is natural, and the multiplication is defined as

$$\forall u, v \in R[G],\ g \in G, \quad (uv)(g) := \sum_{g_1 g_2 = g} u(g_1)v(g_2) = \sum_{s \in g} u(s)v(s^{-1}g).$$

Furthermore, if $R = K$ is a field, then $K[G]$ has a structure of vector spaces, which is called a group algebra.

## Set VII: Modules

1. How does one prove the structure theorem for modules over PID? What is the module and what is the PID in the case of abelian groups?

2. If $M$ is free abelian, how can I put quotients of $M$ in some standard form? What was crucial about the integers here (abelian groups being modules over $\mathbb{Z}$)? How does the procedure simplify if the ring is a Euclidean domain, not just a PID?

3. Suppose $D$ is an integral domain and the fundamental theorem holds for finitely-generated modules over $D$ (i.e. they are all direct sums of finitely many cyclic modules). Does $D$ have to be a PID?

4. Classify finitely-generated modules over $\mathbb{Z}$, over PID, and over Dedekind rings.

5. Prove a finitely-generated torsion-free abelian group is free abelian.

6. What is a tensor product? What is the universal property? What do the tensors look like in the case of vector spaces?

7. Now we'll take the tensor product of two abelian groups, that is, $\mathbb{Z}$-modules. Take $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/q\mathbb{Z}$, where $p$ and $q$ are distinct primes. What is their tensor product?

   *Proposition.* For ideals $I, J$ in $R$, there is a unique $R$-module isomorphism

   $$R/I \otimes_R R/J \longrightarrow R/(I+J)$$
   $$\overline{x} \otimes \overline{y} \longmapsto \overline{xy}.$$

   In particular, for $a, b \in \mathbb{N}$ with $(a, b) = d$, we have $\mathbb{Z}/a\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/b\mathbb{Z} = \mathbb{Z}/d\mathbb{Z}$ as $\mathbb{Z}$-modules (i.e., abelian groups). Also in particular, if $I = J = 0$, then $R \otimes_R R \cong R$.

   *Answer.* In this case, $I = (p), J = (q)$ are coprime ideals, hence $I + J = (1)$ and then $\mathbb{Z}/p\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/q\mathbb{Z} = 0$.

8. What is a projective module?

   *Answer.* The Hom functor $\mathrm{Hom}(M, \cdot)$ is automatically left-exact. It is right-exact iff $M$ is a projective module. This can be defined by universal property as well.

9. What is an injective module?

   *Answer.* The Hom functor $\mathrm{Hom}(\cdot, M)$ is automatically left-exact. It is right-exact iff $M$ is an injective module. This can be defined by universal property as well.

10. Do you know an example of a flat module?

    *Answer.* Recall that the tensoring functors $(\cdot) \otimes M$, $M \otimes (\cdot)$ are naturally right-exact. They become left-exact iff $M$ is a flat module. For some ring $A$, the localization functor on $A$ is exact so that $S^{-1}A$ is always flat over $A$. All projective modules, such as $\mathbb{Z}/6\mathbb{Z}$, are flat (but not necessarily faithfully flat).

## Set VIII: Representation Theory

1. Define "representation" of a group. Define "irreducible representation". Why can you decompose representations of finite groups into irreducible ones? Construct an invariant inner product.

   *Definition.* Group representations describe abstract groups in terms of vector space automorphisms; in particular, the group operation can be represented by matrix multiplication. An irreducible representation has no proper subrepresentations.

   *Answer.* Representations are decomposable because we are working over an algebraically closed field $\mathbb{C}$, such that every matrix in $\mathrm{GL}_n(\mathbb{C})$ turns into blocks. If we are working over $K$ such that $\mathrm{char}(K) = p \nmid |G|$, we can use Maschke's theorem.

   *Construction.* Let $V$ be a finite-dimensional $\mathbb{C}$-vector space with a representation of $G$ on it. Taking any Hermitian inner product $\langle \cdot, \cdot \rangle$ on $V$ and then

   $$\langle v, v' \rangle_G = \frac{1}{|G|} \sum_{g \in G} \langle g(v), g(v') \rangle$$

   is invariant under the action of $G$.

   *Caveat.* There is no modification of this over general characteristic-$p$-field for proving Maschke's theorem. Because a nondegenerate bilinear form gives only orthogonality but cannot guarantee the existence of set-theoretical complement.

2. State and prove Maschke's theorem. What can go wrong if you work over the real field? What can go wrong in characteristic $p$?

   *Statement.* Let $V$ be a finite-dimensional $k$-vector space with a representation of $G$ attached to. If $\mathrm{char}\, k \nmid |G|$, then each $k[G]$-submodule $W$ of $V$ has a complement $k[G]$-submodule, say $W'$ such that $V = W \oplus W'$.

   *Proof.* The upshot is to note that $f : V \to V$ such that

   $$f(v) = \frac{1}{|G|} \sum_{g \in G} g(\mathrm{pr}(g^{-1}(v)))$$

   is a $G$-invariant and $k$-linear automorphism on $V$, where $\mathrm{pr} : V \to W$ is the natural projection. It satisfies $f^2 = f$, and by setting $W' = \mathrm{Ker}\, f$, we obtain $V = W \oplus W'$.

   *Generalization.* Under the same assumption, the group algebra $k[G]$ is semisimple.

   *Answer.* If $k$ is a non-algebraically closed field such as $\mathbb{R}$, the general version must be more complicated: the group algebra $k[G]$ is a product of matrix algebras over division rings over $k$. The summands correspond to irreducible representations of $G$ over $k$. Note that an $\mathbb{R}$-irreducible representation is possibly non-irreducible over $\mathbb{C}$.

   If $\mathrm{char}\, k = p \mid |G|$, it turns out that $|G| = 0$ and $f$ is not constructible. In fact, some subrepresentation does not have a complement here.

3. Do you know what a group representation is? Do you know what the trace of a group representation is?

   *Answer.* A group representation is a group homomorphism $f : G \to \mathrm{GL}(V)$ together with a $k$-vector space (generally $k = \mathbb{C}$). The character of a representation is realized as the trace of image matrices of group elements.

4. State/prove/explain Schur's lemma.

   *Statement.* Let $V$ be a finite-dimensional irreducible representation of $G$ over some field $k$. Then $\mathrm{End}_G(V)$ is a finite-dimensional division algebra over $k$ (i.e., its nonzero elements are all isomorphisms).

   In particular, every linear automorphism on $V$ that is irreducible over $\mathbb{C}$, commuting with $G$-actions, must be a scalar.

   *Proof.* For any $f \in \mathrm{End}_G(V)$, the condition that $f$ commutes with $G$-actions means both $\mathrm{Ker}\, f$ and $\mathrm{im}\, f$ are $G$-invariant. Since $V$ is irreducible,

   $$\begin{aligned} \text{either} \quad & \mathrm{Ker}\, f = 0,\ \mathrm{im}\, f = V \quad \Longrightarrow \quad f \text{ is injective;} \\ \text{or} \quad & \mathrm{Ker}\, f = V,\ \mathrm{im}\, f = 0 \quad \Longrightarrow \quad f = 0. \end{aligned}$$

   If $f$ is injective, it is naturally an isomorphism due to dimension reasons.

   *Note.* The endomorphism algebra $\mathrm{End}_G(V)$ is defined as the vector space of linear automorphisms on $V$ that commute with $G$-actions, i.e.,

   $$\mathrm{End}_G(V) := \{f : V \to V : \rho(g) \circ f = f \circ \rho(g), \forall g \in G\}.$$

   where $\rho : G \to \mathrm{GL}(V)$ is the representation attached to $V$.

   A division algebra over $k$ is a $k$-vector space and also a division ring, in which every nonzero element has a multiplicative inverse.

5. What can you say about characters? What are the orthogonality relations? How do you use characters to determine if a given irreducible representation is a subspace of another given representation?

   *Answer.* Characters are defined as traces of images of $g \in G$ under the representation $\rho : G \to \mathrm{GL}(V)$. All characters of $G$ form a $\mathbb{C}$-vector space, which is equipped with an inner product

   $$\langle \chi, \psi \rangle_G = \sum_{g \in G} \chi(g)\psi(g)^*.$$

   Here $\psi(g)^* = \psi(g^{-1})$ is the complex conjugation. It turns out that the characters of irreducible rep-classes of $G$ form an orthonormal basis, i.e.,

   - $V$ is an irreducible representation with character $\chi$ if and only if $\langle \chi, \chi \rangle_G = 1$;
   - two representations are isomorphic if and only if they obtain the same character;
   - if $\chi, \psi$ are characters of two non-isomorphic representations, then $\langle \chi, \psi \rangle_G = 0$.

   If $(W, \psi)$ and $(V, \chi)$ are given as two reps of $G$, then $W$ is isomorphic to some subrep of $V$ if and only if $\langle \psi, \chi \rangle_G \geqslant 1$, which means it has positive multiplicity in $V$.

6. What's the relation between the number of conjugacy classes in a finite group and the number of irreducible representations?

   *Answer.* They are the same (hence the character table is a square).

   *Proof.* Consider the dimension of $Z(\mathbb{C}[G])$, the space of class functions on $G$. Then $\dim_{\mathbb{C}} Z(\mathbb{C}[G])$ is the number of irreducible representations of $G$. This is because any class function is a $\mathbb{C}$-linear combination of characters for irreducible representations. On the other hand, any class function has constant values on conjugacy classes (by definition). Therefore, this dimension also equals to the number of conjugacy classes.

7. What is the character table? What field do its entries lie in?

   *Answer.* The rows of character table are labeled by irreducible characters (corresponding to irreducible rep-classes). The columns are labeled by conjugacy classes of $G$. It sorts out the values of characters at each conjugacy class. Its entries lie in $\mathbb{C}$ (or more generally, the algebraically closed base field of $V$).

   *Note.* In a character table, no two rows or columns are completely the same. It meant to say that: the valuations at all conjugacy classes uniquely determine an irreducible character; two group elements are conjugate if and only if they have same values under all irreducible characters.

8. Why is the character table a square?

   *Answer.* See Question 6.

9. If $\chi(g)$ is real for every character $\chi$, what can you say about $g$?

   *Answer.* Working over $\mathbb{C}$, this means $\chi(g) = \chi(g)^* = \chi(g^{-1})$ for any irreducible $\chi$. From Question 7, this is equivalent to saying $g$ and $g^{-1}$ are conjugate.

10. What's the regular representation?

    *Answer.* The group algebra $\mathbb{C}[G]$ has a basis $\{e_s\}_{s\in G}$ (see Question 52 in Set VI for the definition), where $e_s$ vanishes outside $s$ and $e_s(s) = 1$. Then $G$ has a left (resp. right) action

    $$\begin{aligned} G \times \mathbb{C}[G] &\longrightarrow \mathbb{C}[G] \\ (g, e_s) &\longmapsto e_{gs} \quad (\text{resp. } e_{sg^{-1}}). \end{aligned}$$

    Consider the left one, and we get $\rho : G \to \mathrm{GL}(\mathbb{C}[G])$ such that $\rho(g)(e_s) = e_{gs}$. This is the so-called regular representation. Its character $\chi_{\mathrm{reg}}(g) = 0$ for $g \neq 1$, and $\chi_{\mathrm{reg}}(1) = |G|$.

    *Punchline.* It turns out that the irreducible decomposition of all regular representations gives all $G$-representation classes up to isomorphisms.

11. Give two definitions of "induced representation". Why are they equivalent?

    *Answer.* There are two algebraic constructions for induced representations. Let $H$ be a subgroup of $G$ with $(\pi, V)$ a given representation on it.

    (I) Say $n = [G : H]$ and $G/H = \{\overline{g}_1, \ldots, \overline{g}_n\}$ are all representatives of left cosets, that is, $\overline{g}_i = g_i H$. Then

    $$\mathrm{Ind}_H^G V := \bigoplus_{i=1}^{n} \overline{g}_i V,$$

    where $\overline{g}_i V = \{\overline{g}_i v, v \in V\}$ is an isomorphic copy of $V$.

    (II) Any representation $(\pi, V)$ of $H$ is regarded as a $K[H]$-module over the group algebra. Then

    $$\mathrm{Ind}_H^G \pi := K[G] \otimes_{K[H]} V$$

    is naturally a $K[G]$-module.

They are equivalent because when $(\pi, V)$ is given, $\mathrm{Ind}_H^G \pi$ and $\mathrm{Ind}_H^G V$ can be mutually determined.

*Note.* The induced representation has a universal property: there is an $H$-equivariant map $f : V \to \mathrm{Ind}_H^G V$ such that for any $H$-equivariant $\psi : V \to \hat{V}$, there is a $G$-equivariant $\varphi : \mathrm{Ind}_H^G V \to \hat{V}$ such that $\psi = \varphi \circ f$.

12. If you have a representation of $H$, a subgroup of a group $G$, how can you induce a representation of $G$?

*Answer.* See Question 11 for the definition of induced representations.

13. If you have an irreducible representation of a subgroup, is the induced representation of the whole group still irreducible?

*Answer.* Typically not. But the restricted representation is always irreducible if the primitive one is.

*Theorem.* (Mackey's Irreducibility Criterion) $\mathrm{Ind}_H^G V$ is irreducible if and only if:

- $V$ is irreducible;
- for any $g \in G - H$, $V$ and $V^g$ has no common irreducible component restricting to $H \cap H^g$. Here $V^g$ is the conjugate representation of $H^g = gHg^{-1}$.

*Counterexample.* Inducing a restriction of some irreducible representation (which is still irreducible) outputs some copies of the original representation.

14. What can you say about the kernel of an irreducible representation? How about kernels of direct sums of irreducibles? What kind of functor is induction? Left or right exact?

*Answer.* The kernel of $\pi : G \to \mathrm{GL}(V)$ must be a normal subgroup of $G$ if $\pi$ is irreducible. Consider the algebra homomorphism

$$\mathbb{C}[G] \longrightarrow \bigoplus_{\pi \text{ irred}} \mathrm{End}(V)$$

where the direct sum goes through all irreducible representations. This is morally a one-to-one correspondence and the kernel must be trivial. Namely, the kernel of some direct sum of different irreducible representations is trivial.

The induction functor, say

$$\begin{aligned} \mathrm{Ind}_H^G : \mathsf{Rep}(H) &\longrightarrow \mathsf{Rep}(G) \\ V &\longmapsto \mathbb{C}[G] \otimes_{\mathbb{C}[H]} V, \end{aligned}$$

is essentially a tensor product (as a left-adjoint of restriction functor, which is exact). Hence $\mathrm{Ind}_H^G$ is always right-exact.

15. What is Frobenius reciprocity?

*Answer.* For any group $G$, there is an inner product $\langle \cdot, \cdot \rangle$ on the vector space of class functions $G \to \mathbb{C}$. Let $H$ be a subgroup and $\varphi : G \to C$, $\psi : H \to C$ be two class functions. Then

$$\langle \mathrm{Ind}_H^G \psi, \varphi \rangle_G = \langle \psi, \mathrm{Res}_H^G \varphi \rangle_H.$$

In other words, the functors $\mathrm{Ind}_H^G$ and $\mathrm{Res}_H^G$ are Hermitian adjoint.

16. Given a normal subgroup $H$ of a finite group $G$, we lift all the representations of $G/H$ to representations of $G$. Show that the intersection of the kernels of all these representations is precisely $H$. What can you say when $H$ is the commutator subgroup of $G$?

    *Proof.* Since all irreducible representations of $G/H$ constitute the regular representation of $G/H$, it suffices to consider $\mathrm{Ind}_{G/H}^{G}\mathrm{reg}$. But its kernel is exactly $H$.

    *Answer.* When $H = [G, G]$ is the commutator subgroup, $G/H$ is abelian and every irreducible representation of it is 1-dimensional. The liftings of these characters to $G$ are decomposed into $\rho_H \otimes \chi_{G/H}$ and $H$ equals the intersection of all $\mathrm{Ker}\,\rho_H$.

17. If you have two linear representations $\pi_1$ and $\pi_2$ of a finite group $G$ such that $\pi_1(g)$ is conjugate to $\pi_2(g)$ for every $g$ in $G$, is it true that the two representations are isomorphic?

    *Answer.* Yes. This condition guarantees $\pi_1(g)$ and $\pi_2(g)$ have the same trace, hence $\chi_1(g) = \chi_2(g)$ for all $g \in G$ at the level of characters. This is equivalent to saying $\pi_1, \pi_2$ are isomorphic.

18. What's special about using $\mathbb{C}$ in the definition of group algebra? Is it possible to work over other fields? What goes wrong if the characteristic of the field divides the order of the group?

    *Answer.* Because $\mathbb{C}$ is an algebraically closed field of characteristic 0 (not dividing $|G|$). The most significant advantage is there is a Hermitian inner product of characters over $\mathbb{C}$.

    If we're using an algebraically closed field $k \neq \mathbb{C}$, all proofs with respect to inner products should be modified. If we're working over non-algebraically closed fields, e.g. the normality of characters in $Z(k[G])$ fails (but the orthogonality still holds).

    Consider the case where $\mathrm{char}(k) \mid |G|$, this leads to the failure of Maschke's theorem hence the group algebra $k[G]$ is possibly not semisimple.

19. Suppose you have a finite $p$-group, and you have a representation of this group on a finite-dimensional vector space over a finite field of characteristic $p$. What can you say about it?

    *Answer.* In this case, any irreducible representation should be trivial. Therefore, any representation is copies of trivial ones.

    *Proof.* Let $V$ be the irreducible finite-dimensional representation space of the given $p$-group over $\mathbb{F}_p$. Consider the action of $G$ on $V^\times = V - \{0\}$. By the orbit-stabilizer formula, for any $v \in V^\times$, the size for the orbit of $v$ must be a power of $p$. On the other hand, the sum of these orbit should be $p^{\dim V} - 1$ since $V$ is defined over $\mathbb{F}_p$. But a sum of powers of $p$ cannot equal to $p^{\dim V} - 1$ unless $\dim V = 0$. Hence $V$ is trivial.

20. Let $(\pi, V)$ be a faithful finite-dimensional representation of $G$. Show that, given any irreducible representation of $G$, the $n$-th tensor power of $\mathrm{GL}(V)$ will contain it for some large enough $n$.

    *Proof.* This statement is known as the **tensor power trick**. It follows from the fact that any irreducible representation of $G$ is a constituent of the regular representation

of $G$. The regular representation can be realized as a subrepresentation of $\mathrm{GL}(V)^{\otimes|G|}$, where $|G|$ denotes the order of $G$. Thus, any irreducible representation of $G$ can be realized as a subrepresentation of $\mathrm{GL}(V)^{\otimes n}$ for some large enough $n$.

21. What are the irreducible representations of finite abelian groups?

*Answer.* In an abelian group $G$, each element $g \in G$ forms a single conjugacy class. Hence there are $|G|$ irreducible representation classes up to isomorphisms. By $|G| = m_1^2 + \cdots m_{|G|}^2 < \infty$, each multiplicity $m_i = 1$, which shows each irreducible representation of a finite abelian group is 1-dimensional. In fact, $G$ has a faithful irreducible representation if and only if $G$ is cyclic.

22. What are the group characters of the multiplicative group of a finite field?

*Answer.* The group $\mathbb{F}_q^\times$ is cyclic of order $q-1 = p^r - 1$ for some prime $p$. Then each $x \in \mathbb{Z}/(q-1)\mathbb{Z}$ forms a single conjugacy class. There are $q-1$ of them, say $C_0, \ldots, C_{q-2}$, and hence there are irreducible characters $\chi_0, \ldots, \chi_{q-2}$ such that

$$\chi_i(C_j) = \zeta_{q-1}^{ij}.$$

*Note.* This construction gives a canonical way to construct characters of cyclic groups.

23. Are there two nonisomorphic groups with the same representations?

*Answer.* Yes. Two groups whose all irreducible representations are the same means equivalently that they share the same character table. For example, $Q_8$ and $D_4$ do this. See Question 26 for the table.

24. If you have a $\mathbb{Z}/5\mathbb{Z}$ action on a complex vector space, what does this action look like? What about an $S_3$ action? A dihedral group of any order?

*Answer.* It can be realized as a rotation on some regular pentagon in $\mathbb{C}^r$ for $r \geqslant 2$. Also, $S_3$ acts on an equilateral triangle and $D_n$ acts on an regular $n$-gon with rotations and reflexions.

25. What are the representations of $S_3$? How do they restrict to $S_2$?

*Answer.* There are 3 conjugacy classes in $S_3$, and hence there are 3 irreducible representations. The character tables for $S_3$ and its restriction to $S_2$ are in the following.

| $S_3$ | $1$ | $(123)$ | $(12)$ |
|---|---|---|---|
| $\chi_0$ | $1$ | $1$ | $1$ |
| $\chi_1$ | $1$ | $1$ | $-1$ |
| $\chi_2$ | $2$ | $-1$ | $0$ |

| $S_2$ | $1$ | $(12)$ |
|---|---|---|
| $\mathrm{Res}^{S_3}_{S_2}\chi_0$ | $1$ | $1$ |
| $\mathrm{Res}^{S_3}_{S_2}\chi_1$ | $1$ | $-1$ |

*Example.* Here comes an explicit construction of the irreducible representation $\pi_2$ for irreducible character $\chi_2$. Note that $S_3 \cong \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, so

$$S_3 = \langle x, y : x^3 = y^2 = 1, yx = x^{-1}y \rangle, \quad x = (123), \quad y = (12).$$

One may take

$$X = \begin{pmatrix} \zeta_3 & 0 \\ 0 & \zeta_3^{-1} \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

such that the representation $\pi_2 : S_3 \to \mathrm{GL}_2(\mathbb{C})$ sends $x \mapsto X$, $y \mapsto Y$. One can check that $\chi_2(x) = \zeta_3 + \zeta_3^{-1} = -1$, and $\chi_2(y) = 0$. Since $\chi_1, \chi_2$ restrict to $S_2 = \{1, y\}$, this $\pi_2$ has only trivial restriction to $S_2$.

26. Tell me about the representations of $D_4$. Write down the character table. What is the 2-dimensional representation? How can it be interpreted geometrically?

*Notes.* In a character table, if all but one characters are already obtained, there are 3 different approaches to compute the last one:

- using the equality $\chi_{\mathrm{reg}} = \sum m_i \chi_i$;
- using the column orthogonality relation, i.e., for conjugacy classes $C_0, \ldots, C_n$,
$$\chi_0(C_i)\chi_0(C_j)^* + \cdots + \chi_n(C_i)\chi_n(C_j)^* = 0, \quad i \neq j;$$
$$\chi_0(C_i)\chi_0(C_i)^* + \cdots + \chi_n(C_i)\chi_n(C_i)^* = g/|C_i|.$$
- computing it as an induced representation from some subgroup:
$$(\mathrm{Ind}_H^G \chi)(x) = \sum_{g_i \in G/H} \chi(g_i x g_i^{-1})$$
for $x \in G$ and all representatives $g_i$ of $G/H$.

*Solution.* By definition,
$$D_4 = \langle x, y : x^4 = y^2 = 1, yxy^{-1} = x^{-1} \rangle.$$
We first compute $D_4^{\mathrm{ab}} = D_4/[D_4, D_4]$: since $[x, y] = xyx^{-1}y^{-1} = x^2$, and if $x^2 = 1$ then $yxy^{-1} = x^{-1} = x$ (i.e., $x, y$ mutually commutes), we get $[D_4, D_4] = \langle x^2 \rangle$; now $|D_4^{\mathrm{ab}}| = 4$, which is the number of 1-dimensional irreducible representations. On the other hand, $D_4$-action has a 2-dimensional geometric realization, so there is one 2-dimensional irreducible representation. Note that all 5 conjugacy classes in $D_4$ are given by
$$\{1\}, \{x, x^3\}, \{y, x^2y\}, \{x^2\}, \{xy, x^3y\}.$$
In the following character table, $\chi_0, \ldots, \chi_3$ permutes $\pm 1$ over $x$ and $y$, and there are 3 different ways to determine $\chi_4$: using the $\chi_{\mathrm{reg}}$, using the column orthogonality, and computing it as an induce representation from the subgroup $\langle x \rangle$.

| $D_4$ | $1$ | $x$ | $y$ | $x^2$ | $xy$ |
|---|---|---|---|---|---|
| $\chi_0$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_1$ | 1 | −1 | 1 | 1 | −1 |
| $\chi_2$ | 1 | 1 | −1 | 1 | −1 |
| $\chi_3$ | 1 | −1 | −1 | 1 | 1 |
| $\chi_4$ | 2 | 0 | 0 | −2 | 0 |

*Interpretation.* Since $D_4$ has only one 2-dimensional irreducible representation, this can be viewed as the action of $D_4$ on a rectangle in $\mathbb{C}^2$. Hence $D_4 \to \mathrm{GL}_2(\mathbb{C})$ is constructed. Here $r$ is represented by the rotation by 90°, and $s$ is represented by the reflection whose axis doesn't go through any vertices.

*Remark.* Any dihedral group $D_n$ generally admits this interpretation on $\mathbb{C}^2$, hence the 2-dimensional irreducible representation always exists for $D_n$ (and the number of them is morally $n/2 - 1$). See Question 27 below.

27. How would you work out the orders of the irreducible representations of the dihedral group $D_n$? Why is the the sum of squares of dimensions equal to the order of the group?

*Answer.* Say $D_n = \langle r, s : r^n = s^2 = 1, srs^{-1} = r^{-1} \rangle$. Then any element in $D_n$ can be written in the form $r^k$ or $sr^k$ for $0 \leqslant k \leqslant n-1$.

(I) The case $2 \mid n$. Corresponding $\pm 1$ with $r$ and $s$ alternatively, we get 4 irreducible linear characters:

| | $r^k$ | $sr^k$ |
|---|---|---|
| $\psi_1$ | $1$ | $1$ |
| $\psi_2$ | $1$ | $-1$ |
| $\psi_3$ | $(-1)^k$ | $(-1)^k$ |
| $\psi_4$ | $(-1)^k$ | $(-1)^{k+1}$ |

Consider 2-dimensional representations. One can define $\rho_j : D_n \to \mathrm{GL}_2(\mathbb{C})$ by

$$\rho_j(r^k) = \begin{pmatrix} \zeta_n^{jk} & 0 \\ 0 & \zeta_n^{-jk} \end{pmatrix}, \quad \rho_j(sr^k) = \begin{pmatrix} 0 & \zeta_n^{-jk} \\ \zeta_n^{jk} & 0 \end{pmatrix}$$

that correspond to character $\chi_j$. Note that $\chi_0 = \psi_1 + \psi_2$ and $\chi_{n/2} = \psi_3 + \psi_4$ (here $\rho_j = \rho_{n-j}$, we may assume $0 < j < n/2$). Also,

$$\chi_j(r^k) = \zeta_n^{jk} + \zeta_n^{-jk} = 2\cos(\frac{2\pi}{n} jk), \quad \chi_j(sr^k) = 0.$$

Hence there are 4 irreducible 2-dimensional representations and $n/2 - 1$ irreducible 2-dimensional representations.

(II) The case $2 \nmid n$. There are only 2 irreducible linear characters: $\psi_1, \psi_2$ as before. The remaining constructions are the same. It turns out to have $(n-1)/2$ irreducible 2-dimensional representations.

**Check:** Since he sum of squares of dimensions equal to the order of the group, there are no more irreducible representations. This fact holds because

$$|G| = \chi_{\mathrm{reg}}(1) = \sum m_i \chi_i(1) = \sum m_i^2.$$

28. What about representations of $A_4$? Give a nontrivial one. What else is there? How many irreducible representations do we have? What are their degrees? Write the character table of $A_4$.

*Solution.* Symmetries of a tetrahedron form a nontrivial representation of $A_4$. Since $V \triangleleft A_4$, there is a 2-dimensional (non-irreducible) representation whose kernel is $V \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$:

| Cosets of $V$ in $A_4$ | Representation Images |
|---|---|
| $\{(1), (12)(34), (13)(24), (14)(23)\}$ | $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ |
| $\{(123), (243), (142), (134)\}$ | $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ |
| $\{(132), (234), (124), (143)\}$ | $\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$ |

Note that $A_4$ admits a doubly transitive action on $\{1,2,3,4\}$ such that the standard representation gives an irreducible character of degree 3, say $\chi_3$. In the following, $\chi_1$ and $\chi_2$ are linear and they can be determined by orthogonality relations.

| $A_4$ | (1) | (12) | (123) | (132) |
|---|---|---|---|---|
| $\chi_0$ | 1 | 1 | 1 | 1 |
| $\chi_1$ | 1 | 1 | $\omega$ | $\omega^2$ |
| $\chi_2$ | 1 | 1 | $\omega^2$ | $\omega$ |
| $\chi_3$ | 3 | $-1$ | 0 | 0 |

29. Write the character table for $S_4$.

*Recipe.* While computing characters of $G$ that acts double-transitively on some set $X$, an irreducible character can be attained by taking the number of fixed points (of each representatives) and subtracting 1. Also, there is a nontrivial sign-character by taking $-1$ at all transitions on $S_n$. Using the following lemma, we can get some $\chi\theta$ with $\deg \chi\theta > 1$ from $\chi$ for free: "linear $\times$ irreducible = irreducible".

*Lemma.* If $\chi$ is a character and $\theta$ is a linear character, then $\chi\theta$ is a character, and is irreducible if and only if $\chi$ is.

*Solution.* Say $S_4$ has 5 conjugacy classes:

$$\begin{aligned}
C_0 &= \{(1)\},\\
C_1 &= \{(12),(13),(14),(23),(24),(34)\},\\
C_2 &= \{(123),(132),(213),(231),(312),(321)\},\\
C_3 &= \{(1234),(1243),(1324),(1342),(1423),(1432)\},\\
C_4 &= \{(12)(34),(13)(24),(14)(23)\}.
\end{aligned}$$

In the character table, $\chi_1$ is given by alternating signs on $A_4$. And $\chi_3$ is given by "#{fixed points} $-$ 1". Then we get irreducible $\chi_4 = \chi_1\chi_3$ for free. Finally, from the regular character, $\deg \chi_2 = 2$ and $2\chi_2 = \chi_{\text{reg}} - \chi_0 - \chi_1 - 3\chi_3 - 3\chi_4$.

| $S_4$ | (1) | (12) | (123) | (1234) | (12)(34) |
|---|---|---|---|---|---|
| $\chi_0$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_1$ | 1 | $-1$ | 1 | $-1$ | 1 |
| $\chi_2$ | 2 | 0 | $-1$ | 0 | 2 |
| $\chi_3$ | 3 | 1 | 0 | $-1$ | $-1$ |
| $\chi_4$ | 3 | $-1$ | 0 | 1 | $-1$ |

30. Start constructing the character table for $S_5$.

*Sketchy Solution.* Say $S_5$ has 7 different conjugacy classes:

| Representatives | (1) | (12) | (12)(34) | (123) | (12)(345) | (12345) | (1234) |
|---|---|---|---|---|---|---|---|
| Size of Classes | 1 | 10 | 15 | 20 | 20 | 24 | 30 |
| Size of Centralizers | 120 | 12 | 8 | 6 | 6 | 5 | 4 |

In the following character table, $\chi_1$ is the sign character and $\chi_2$ is the standard character, i.e., the natural representation on $\{1,2,3,4,5\}$ subtracting $\chi_0$. From these we get $\chi_3 = \chi_2\chi_1$ by "linear $\times$ irreducible = irreducible". From orthogonality on rows and columns (see Question 26), we can completely determine $\chi_4$, $\chi_5 = \chi_4\chi_1$, and $\chi_6$ (given by $\chi_{\text{reg}}$).

| | 1 | (12) | (12)(34) | (123) | (123)(45) | (12345) | (1234) |
|---|---|---|---|---|---|---|---|
| $\chi_0$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $\chi_1$ | 1 | $-1$ | 1 | 1 | $-1$ | 1 | $-1$ |
| $\chi_2$ | 4 | 2 | 0 | 1 | $-1$ | $-1$ | 0 |
| $\chi_3$ | 4 | $-2$ | 0 | 1 | 1 | $-1$ | 0 |
| $\chi_4$ | 5 | $-1$ | 1 | $-1$ | $-1$ | 0 | 1 |
| $\chi_5$ | 5 | 1 | 1 | $-1$ | 1 | 0 | $-1$ |
| $\chi_6$ | 6 | 0 | $-2$ | 0 | 0 | 1 | 0 |

31. How many irreducible representations does $S_n$ have? What classical function in mathematics does this number relate to?

*Answer.* See Question 18 in Set I for conjugacy classes in $S_n$. The number of irreducible representations is the number of partitions $\lambda = (\lambda_1, \ldots, \lambda_m)$ for $n$, where $\lambda_i \geqslant \lambda_{i+1}$ and $\lambda_1 + \cdots + \lambda_m = n$. This is given by the partition function, which doesn't have an explicit expression. Young diagrams are useful in computing this function.

32. Discuss representations of $\mathbb{Z}$, the infinite cyclic group. What is the group algebra of $\mathbb{Z}$? What is the connection with modules over PIDs? When is a representation of $\mathbb{Z}$ completely reducible? Why not always? Which are the indecomposable modules?

*Answer.* Every infinite cyclic group is isomorphic to $\mathbb{Z}$. Each representation $\rho : \mathbb{Z} \to \mathrm{GL}(V) = \mathrm{GL}_1(\mathbb{C})$ is determined by $\rho(1) \in \mathbb{C}$. So each such $\rho$ is characterized by a complex number $\rho(1) = z$. The group algebra

$$\mathbb{C}[\mathbb{Z}] = \left\{ \sum_{n\in\mathbb{Z}} n a_n \in \mathbb{C} : a_i \in \mathbb{C},\ a_i = 0 \text{ for all but finitely many } i \in \mathbb{Z} \right\}.$$

33. State Artin's theorem and Brauer's theorem.

*Artin's Theorem.* Let $k$ be a field of characteristic 0 (but not necessarily algebraically closed) and $G$ be any group. Let $X$ be a set of subgroups in $G$. Consider the map

$$\mathrm{Ind}_X = \bigoplus_{H\in X} \mathrm{Ind}_H^G : \mathsf{Rep}(H) \to \mathsf{Rep}(G)$$

between representations over $k$. Then the following are equivalent:

(1) Up to conjugation, $G$ can be set-theoretically covered by subgroups in $X$, i.e.

$$G = \bigcup_{H\in X} \bigcup_{g\in G} gHg^{-1}.$$

(2) The map $\mathrm{Ind}_X \otimes_{\mathbb{Z}} \mathbb{Q}$ is surjective. That is, for any $\rho \in \mathsf{Rep}(G)$, there exist an integer $d \geqslant 1$ and $\rho_H \in \mathsf{Rep}(H)$ for each $H \in X$, such that

$$d \cdot \rho = \sum_{H\in X} \mathrm{Ind}_H^G \rho_H.$$

*Conventions.* Let $p$ be a prime number. A finite group $H$ is called *$p$-elementary* if $H = C \times P$, where $C$ is a cyclic group with prime-to-$p$ order and $P$ is a $p$-group. Denote $X(p)$ the set of all $p$-elementary subgroups of $G$.

*Brauer's Theorem.* Suppose further $k$ is algebraically closed of characteristic 0 and $G$ is a finite group. If $X$ is the union of all the $X(p)$ for $p$ prime, then $\mathrm{Ind}_X$ is surjective.

34. What is a Lie group? What is the Lie algebra? How do you get from a Lie algebra to a Lie group? The Jacobi identity?

*Definition.* A Lie group is a topological group $G$ (such that the operation and the inverse function are smooth) that is a smooth manifold as well.

A Lie algebra is a vector space $\mathfrak{g}$ equipped with a bilinear map $[\cdot,\cdot]$, say Lie bracket, satisfying $[x,x]=0$ and the Jacobi identity: $[x,[y,z]]+[y,[z,x]]+[z,[x,y]]=0$ for all $x,y,z\in\mathfrak{g}$.

*Answer.* Given $\mathfrak{g}$, embed it as a subalgebra of $\mathfrak{gl}_n$ and then exponentiate to get $G$ as a subgroup of $\mathrm{GL}_n$.

35. Define a unitary representation. What is the Peter–Weyl theorem?

*Definition.* A representation $(\pi,V)$ of $G$ is unitary if $V$ is a complex Hilbert space and $\pi(g)$ is a unitary operator on $V$ for all $g\in G$.

*Statement.* (Peter–Weyl) Let $\pi$ be a unitary representation of a compact group $G$ on a complex Hilbert space $\mathcal{H}$. Then $\mathcal{H}$ splits into an orthogonal direct sum of irreducible finite-dimensional unitary representations of $G$.

*Corollary.* Every compact Lie group has a faithful finite-dimensional representation and is therefore isomorphic to a closed subgroup of $\mathrm{GL}_n(\mathbb{C})$ for some $n$.

36. What is the adjoint representation of a Lie algebra? What is the commutator of two vector fields on a manifold?

*Answer.* The adjoint representation of a Lie algebra is a way of representing the elements of the Lie algebra as linear transformations of itself. This is done by associating each element $x$ of the Lie algebra with a linear transformation $\mathrm{ad}_x$ defined by $\mathrm{ad}_x(y)=[x,y]$, where $[x,y]$ denotes the Lie bracket of $x$ and $y$.

The commutator of two vector fields on a manifold is another vector field defined by its action on functions. If $X$ and $Y$ are two vector fields on a manifold, then their commutator is given by $[X,Y]f=X(Yf)-Y(Xf)$ for any smooth function $f$ on the manifold.

37. Talk about the representation theory of compact Lie groups. How do you know you have a finite-dimensional representation?

*Answer.* Representation theory of a compact Lie group $G$ is concerned with studying continuous group homomorphisms $G\to\mathrm{GL}(V)$ with $\dim V<\infty$. One important result is the Peter–Weyl theorem (Question 35). Consequently, if we have a continuous homomorphism from $\rho:G\to\mathrm{GL}(W)$ with $\dim W=\infty$, then $\rho$ cannot be irreducible.

38. How do you prove that any finite-dimensional representation of a compact Lie group is equivalent to a unitary one?

*Proof.* For a compact Lie group $G$, we are able to stick an arbitrary inner product $\langle\cdot,\cdot\rangle$ on the given finite-dimensional representation space $V$. Then the average inner

product in Hermitian. To be more precise, for the compact group,

$$\langle x, y\rangle' = \int_G \langle g(x), g(y)\rangle dg.$$

This endows a unitary structure on $G$.

39. Do you know a Lie group that has no faithful finite-dimensional representations?

*Philosophy.* Since every group has a trivial finite-dimensional unitary representation, non-faithful representations (but not necessarily finite-dimensional) are very easy to construct. There have morally been some finite-dimensional ones: the nontrivial covers for $\mathrm{SL}_2(\mathbb{R})$.

*Answer.* Any finite-dimensional Lie algebra $\mathfrak{g}$ can be realized as the algebra of a simply connected universal cover Lie group $\widetilde{G}$. Recall that

$$\mathrm{Hom}(G, H) \longrightarrow \mathrm{Hom}(\mathfrak{g}, \mathfrak{h})$$

is always injective for connected Lie groups $G, H$, and is bijective if $G$ is simply connected. Then take $G = \mathrm{SL}_2(\mathbb{R})$ and $H = \mathrm{GL}_n(\mathbb{R})$. Now $G$ is a semisimple Lie group with simple Lie algebra $\mathfrak{g} = \mathfrak{sl}_2(\mathbb{R})$. The finite-dimensional representations of $\mathfrak{sl}_2(\mathbb{R})$ are completely reducible, and the irreducible representations of $\mathfrak{sl}_2(\mathbb{R})$ are precisely the symmetric powers $\mathrm{Sym}^n(\mathbb{R}^2)$ of the defining representation. It turns out that every irreducible representation of any nontrivial cover of $G$ factors through the covering map to $G$. It follows that nontrivial covers of $G = \mathrm{SL}_2(\mathbb{R})$ (which exist) have no faithful finite-dimensional representations.

40. What do you know about representations of SO(2)? SO(3)?

*Comment.* The answer should be complicated and we choose to omit. For representation theory of compact Lie groups, it would be worthwhile to completely memorize everything about $\mathrm{SU}(n)$, $\mathrm{SO}(2n)$, $\mathrm{Sp}(n)$, and $\mathrm{SO}(2n+1)$ (i.e. their Lie algebras, maximal tori, Cartan subalgebras, simple roots, positive roots, roots, Weyl chambers, Weyl groups, Dynkin diagrams, etc.).

## Set IX: Categories and Functors

1. Which is the connection between Hom and tensor product? What is this called in representation theory?

   *Answer.* They are a pair of adjoint functors, i.e., in some small category $\mathcal{C}$,

   $$\mathrm{Hom}_{\mathcal{C}}(X \otimes Y, Z) \longrightarrow \mathrm{Hom}_{\mathcal{C}}(X, \mathrm{Hom}(Y, Z)).$$

   This is called **Frobenius reciprocity** in representation theory, which states tensor product as the functor for induced representations and Hom as the functor of restrictions, respectively.

2. Can you get a long exact sequence from a short exact sequence of abelian groups together with another abelian group?

   *Answer.* This is just the long exact sequence of group cohomology. For a (discrete) group $G$, which is not necessarily abelian, acting on another abelian group $M$ (with discrete topology), which is called a $G$-module, we can define $H^i(G, M) := \mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, M)$. This theory is covariant in $M$ and contravariant in $G$.

3. Do you know what the Ext functor of an abelian group is? Do you know where it appears? What is $\mathrm{Ext}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$? What is $\mathrm{Ext}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z})$? How about $\mathrm{Ext}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Q})$?

   *Answer.* The Ext functor is a derived functor that measures the failure of a short exact sequence of modules to split. Also, $\mathrm{Ext}(A, B)$ classifies abelian extensions of $A$ by $B$. It appears in Cartan–Eilenberg's 1956 book *Homological Algebra*.

   *Solution.* For any $\mathbb{Z}$-module $M$, the homomorphism $\mathbb{Z} \to M$ is defined by the image of 1 in $H$. So

   $$\mathrm{Hom}(\mathbb{Z}, M) = M, \quad \mathrm{Ext}(\mathbb{Z}, M) = 0$$

   because $\mathbb{Z}$ is a projective module (c.f. Set 7, Question 8). We begin the computation with a projective resolution of $\mathbb{Z}/m\mathbb{Z}$ as follows:

   $$0 \longrightarrow \mathbb{Z} \xrightarrow{\times m} \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \longrightarrow 0.$$

   Taking the contravariant functor $\mathrm{Hom}(-, M)$, we get

   $$\begin{array}{ccccccc} & & & & M & & M \\ & & & & \| & & \| \\ 0 & \longrightarrow & \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, M) & \longrightarrow & \mathrm{Hom}(\mathbb{Z}, M) & \xrightarrow{\times m} & \mathrm{Hom}(\mathbb{Z}, M) \\ & & & \searrow & & & \\ & & & & \mathrm{Ext}(\mathbb{Z}/m\mathbb{Z}, M) & \longrightarrow & \mathrm{Ext}(\mathbb{Z}, M) = 0. \end{array}$$

   It follows that

   $$\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, M) = \mathrm{Ker}\, m = M[m], \quad \mathrm{Ext}(\mathbb{Z}/m\mathbb{Z}, M) = M/mM.$$

   In particular, $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}) = 0$ and $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/d\mathbb{Z}$ for $d = (m, n)$. Moreover,

   $$\mathrm{Ext}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/d\mathbb{Z}, \quad \mathrm{Ext}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}) = \mathbb{Z}/m\mathbb{Z}.$$

   Also, we have $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Q}) = \mathrm{Ext}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Q}) = 0$.