ALGEBRA QUAL PREP 2025

ANIRUDDHA SUDARSHAN

1. Linear algebra

QUESTION 1.1. What is the characteristic polynomial of $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$?

QUESTION 1.2 (FALL 2024). Let $\mathbb{F}_3$ be the field with 3 elements. and let

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 2 & 2 \\ 2 & 0 & 2 \end{pmatrix} \in M_3(\mathbb{F}_3).$$

(1) Calculate the characteristic polynomial of A.
(2) Find the eigenvalues and eigenspaces (in $\mathbb{F}_3^3$) of A.
(3) What is the minimal polynomial of A? Justify your answer.
(4) Is A diagonalizable over $\mathbb{F}_3$? Over an algebraic closure of $\mathbb{F}_3$? Justify your answer.

QUESTION 1.3 (SPRING 2021). Let V be a finite-dimensional vector space over some field K, let $T \in \operatorname{End}_K(V)$ be a linear operator on V, and let $W \subseteq V$ be a subspace such that $T(W) \subseteq W$. Let m, m_1, and m_2 denote the minimal polynomials of T viewed as an operator on V, W, and V/W (why does T induce a linear operator on V/W?), respectively. Show:

(1) m divides $m_1 m_2$.
(2) If m_1 and m_2 are relatively prime, then $m = m_1 m_2$.
(3) Give an example with $m \neq m_1 m_2$.

QUESTION 1.4 (FALL 2022). Let V be a finite dimensional vector space over a field K, and let $T : V \to V$ be a linear opeartor on V. Consider a family of subspaces $W_i \subseteq V$ (for $i \in I$) such that $T(W_i) \subseteq W_i$ and denote $T_i := T|_{W_i} : W_i \to W_i$. Let m, m_i denote degree of minimal polynomials of T and T_i respectively. Show that

(1) m_i divides m.
(2) If $V = \sum_{i \in I} W_i$, then m is the least common multiple of m_i's.

QUESTION 1.5 (FALL 2021). Let V be a finite-dimensional vector space over the field R with $\dim_R V \geq 3$. Let $T : V \to V$ be a linear operator. Show that there exists a nonzero proper subspace W of V such that $T(W) \subseteq W$.

QUESTION 1.6. Recall that the Cayley–Hamilton Theorem holds for matrices in $M_n(R)$, the ring of $n \times n$ matrices over a commutative ring R. Use this to show that $AB = I_n$ implies $BA = I_n$ for $A, BM_n(R)$, and where I_n is the multiplicative identity of $M_n(R)$.

2. GROUP THEORY

QUESTION 2.1. Let $\mathbb{Q}$ be the group of rational numbers and let $\mathbb{Z}$ be the subgroup of integers. Let G be the group $\{e^{2\pi i\theta} \mid \theta \in \mathbb{Q}\}$ under multiplication. Show that

$$\mathbb{Q}/\mathbb{Z} \cong G.$$

QUESTION 2.2. Let $\mathrm{Aut}(G)$ denote the group of automorphisms of a group G. For $g \in G$, we denote

$$\alpha_g : G \to G, \quad x \mapsto gxg^{-1}.$$

Show that the set $\mathrm{Inn}(G) := \{\alpha_g \mid g \in G\}$ forms a normal subgroup of $\mathrm{Aut}(G)$, called the group of inner automorphisms of G. The quotient $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the group of outer automorphisms of G.

QUESTION 2.3. Let $\gamma = (1\ 2\ \ldots\ n) \in S_n$ be an n-cycle. Show that the conjugacy class of γ in S_n has cardinality $(n-1)!$. Moreover, the centralizer of γ is $C(\gamma) = \langle \gamma \rangle$.

QUESTION 2.4. Let G be a group.

(1) If H, K are subgroups of finite index, then $H \cap K$ has finite index in G.

QUESTION 2.5. Let p be the smallest prime dividing the order of a group G. Show that any subgroup of index p in G is normal.

QUESTION 2.6. Let $D_4 = \langle r, s \mid r^4 = s^2 = 1,\ sr = r^{-1}s \rangle$ be the order 8 dihedral group and let $Q_8 = \langle i, j \mid i^4 = j^2 i^2 = j^{-1}iji = 1 \rangle$ be the group of quaternions.

(1) Show that D_4 is not isomorphic to Q_8.
(2) Show that any non-abelain group of order 8 is isomorphic to one of D_4 or Q_8.
(3) Classify abelian groups of order 8?

QUESTION 2.7. Let S_n be the symmetric group on n letters and G be an abelian subgroup of S_n that acts transitively on set $\{1, 2, \ldots, n\}$.

(1) Prove that the order of the group G is n.
(2) Give an example of an abelian subgroup G of S_n for some n such that G acts transitively on $\{1, 2, \ldots, n\}$ and is not cyclic.

QUESTION 2.8. An abelian group A, written additively, is called divisible if for every non-zero integer $n \in \mathbb{Z}$, and $a \in A$, there is a $b \in A$ such that $a = nb$ ("$b = a/n$"). A is torsion if every $a \in A$ has a finite order. Now, let $A = (\mathbb{Q}, +)$. Prove:

(1) If B is any nonzero subgroup of A, then AB is both divisible and torsion.
(2) A has no proper subgroups of finite index.

QUESTION 2.9. Let F_n denote the free group on n generators. Show that the abelianization of $F_n := F_n/[F_n, F_n]$ is isomormorphic to $\mathbb{Z}^n$. Moreover, show that $F_n \cong F_m$ if and only if $n = m$.

QUESTION 2.10.

(1) Give an example of an infinite abelian group that is also torsion.
(2) Show that an ininite abelian torsion group cannot be finitely generated.

(3) Give an example of a torsion abelian group A and a non-zero subgroup B of A such that $A/B \cong A$.

QUESTION 2.11 (CLASS EQUATION). Let G be a finite group with center C. For an element $g \in G$, denote $C(g)$ for the centralizer of g in G. Show that

$$|G| = |C| + \sum |G/C(g)|,$$

where the sum runs over representatives $g \notin C$ of conjugacy classes.

QUESTION 2.12. Let G be a group of order p^3, where p is prime. Determine all possibilities for the number of conjugacy classes in G and their sizes.

2.1. **Sylow theorems.**

THEOREM 2.13 (SYLOW THEOREMS). *Let G be a finite group of order n and let p be a prime dividing n. Then,*

(1) p-Sylow groups exists.
(2) Any two p-Sylow subgroups are conjugates.
(3) Let $p^e || n$, and let m_p is the number of p-Sylow subgroups. Then

$$m_p | n/p^e \quad \text{and} \quad m_p \equiv 1 \bmod p.$$

QUESTION 2.14 (FALL 2023). Let G be a finite group acting transitively on a set X.

(1) Suppose $|G| = 65$. If g has order 5, and g fixes one element of X, then g fixes every element of X. (Use Sylow theorems)
(2) Show that (1) is false when $|G| = 60$. There is an action of the alternating group A_5 on a set X with $|X| = 6$ so that every 5-cycle in A_5 has a fixed point in X but no 5-cycle fixes every $x \in X$.

QUESTION 2.15 (SPRING 2013). Let G be a group of order p^3q for primes p, q. Show that G is not simple.

Proof. Let n_p, n_q be the number of p, q-Sylow subgroups of G. By Sylow's theorem, $n_p | q$ and $n_q | p^3$. Moreover, $n_p \equiv 1 \bmod p$ and $n_q \equiv 1 \bmod q$. If $n_p = 1$, then we are done. If not, $n_p = q$ and the first equation implies $q > p$. Let H be a subgroup of G of order p^2 (show that this exists) and let K be a subgroup of order q in G. Then, the subsgroup HK is normal since its index is p, the smallest prime dividing G. □

2.2. **Fundamental theorem of abelian groups.**

THEOREM 2.16. *Let G be a finitely generated abelian group. Then,*

$$G = \mathbb{Z}^r \times \left(\frac{\mathbb{Z}}{n_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{n_s\mathbb{Z}} \right),$$

where

(1) $r \geq 0$.
(2) $n_i > 1$ for all i, and $n_i | n_{i-1}$ for all $2 \leq i \leq s$.

Moreover, the above expression satisfying (1) and (2) is unique.

DEFINITION 2.17. The (unique) integer r in the above theorem is called the *rank* (or *Betti number*) of G. The factors $n_1, \dots, n_s$ are called *invariant factors* of G. The above decomposition is called *invariant factor decomposition*.

QUESTION 2.18. If n is square-free (product of distinct primes), then any abelian group of order n is cyclic.

QUESTION 2.19. Classify all abelian groups of order 36.

QUESTION 2.20. Let G be an abelian group of order $n = p_1^{e_1} \cdots p_k^{e_k}$. Let P_k denote the p_k-Sylow subgroup. Show that

$$G = P_1 \times \cdots \times P_k,$$

and for each P_i, there exists invariant factors $p_i^{\beta_{j,i}}$ such that

$$P_i = \frac{\mathbb{Z}}{p_i^{\beta_{1,i}}\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{p_i^{\beta_{t,i}}\mathbb{Z}}.$$

The divisors $p_i^{\beta_{j,i}}$ are called *elementary divisors* of G and the above decomposition is called the *elementary divisor decomposition*.

QUESTION 2.21. Show that the number of abelian groups of order p^n is $P(n)$, the number of partitions of n.

2.3. **Nilpotent and solvable groups.** For a group G, let $Z(G)$ denote its center.

DEFINITION 2.22. Let G be a group. Define $Z_0(G) = 1$ and

$$Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G)), \quad \text{for } i \geq 1.$$

We have the *upper central series*

$$Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \cdots \leq G.$$

The group G is called *nilpotent* if $Z_n(G) = G$ for some $n \geq 1$. The smallest such n is called the *nilpotency class* of G.

Examples.

(1) A non-trivial group has nilpotency class 1 if and only if it is abelian.
(2) Let $G = S_3$, then $Z_i(G) = 1$ for all $i \geq 0$. Hence, S_3 is not nilpotent.

QUESTION 2.23. Show that D_4 and Q_8 are nilpotent of class 2. Moreover, show that D_{2^n} is nilpotent of class $n-1$.

DEFINITION 2.24. Let G be a group. Define $G^0 = G$, and

$$G^i = [G, G^{i-1}], \quad \text{for } i \geq 1.$$

We have the lower central series

$$G^0 \supseteq G^1 \supseteq \cdots.$$

QUESTION 2.25. A group G is nilpotent if and only if there is an $n \geq 1$ such that $G^n = 1$. Moreover, if G is of nilpotency class n, then

$$Z_i(G) \leq G^{n-i-1} \leq Z_{i+1}(G).$$

THEOREM 2.26. *Let G be a finite group, and let $p_1, \ldots, p_k$ be distinct prime divisors of its order. Let P_k be the p_k-Sylow subgroup of G. Then the following are equivalent:*

(1) G is nilpotent.
(2) For a proper subgroup $H < G$, H is a proper subgroup of its normalizer $N(H)$ in G.
(3) Every Sylow subgroup is normal in G.
(4) $G \cong P_1 \times \cdots \times P_k$.

DEFINITION 2.27. A subgroup C of G is said to be *characteristic* if C is fixed by every automorphism of G.

EXAMPLE 2.28. A normal p-Sylow subgroup is characteristic.

QUESTION 2.29 ([DF04], P. 198, EX.1). Show that the groups $Z_i(G)$ are characteristic.

QUESTION 2.30 ([DF04], P. 198, EX.6). If $G/Z(G)$ is nilpotent, then G is nilpotent.

QUESTION 2.31 ([DF04], P. 198, EX.4). Prove that a maximal subgroup of a finite nilpotent group has prime index.

QUESTION 2.32 ([DF04],P. 198, EX. 9, 10). Prove that a finite group G is nilpotent if and only if whenever $a, b \in G$ with coprime orders, then $ab = ba$. Using this, show that D_n (the dihedral group of order $2n$) is nilpotent if and only if n is a power of 2.

DEFINITION 2.33. A group G is *solvable* if there is a series

$$1 < H_1 < \cdots < H_{n-1} < H_n = G$$

such that H_{i-1} is normal in H_i, and H_i/H_{i-1} is abelian.

EXAMPLE 2.34. S_3 is solvable: $1 < \langle (1\ 2\ 3) \rangle < S_3$.

Define the *derived series* of G as follows: Let $G^{(0)} = G$, and

$$G^{(i)} = [G^{(i-1)}, G^{(i-1)}].$$

THEOREM 2.35. *A group G is solvable if and only if $G^{(n)} = 1$ for some $n \geq 1$. The smallest such n is called the* solvable length *of G.*

QUESTION 2.36.

(1) Subgroups of solvable groups are solvable.
(2) Homomorphic image of a solvable group is solvable.
(3) If N is a normal subgroup of G, and both N and G/N is solvable, then G is solvable.

QUESTION 2.37 ([DF04], P. 213, EX. 5). Let G be a solvable group of order pm, where p is a prime not dividing m, and let P be a p-Sylow subgroup of G. If the normalizer $N_G(P)$ of P is equal to P, then prove that G has a normal subgroup of order m. Where was the solvability of G needed in the proof? (This result is true for nonsolvable groups as well - it is a special case of *Burnside's N/C-Theorem*.)

DEFINITION 2.38. An elementary abelian p-group is a group isomorphic to a finite directed sum of $\mathbb{Z}/p\mathbb{Z}$.

QUESTION 2.39 ([DF04], P. 200, EX. 36). Let p be a prime, let V be a nonzero finite dimensional vector space over the field of p elements and let φ be an element of $\mathrm{GL}(V)$ of order a power of p (i.e. V is a nontrivial elementary abelian p-group and φ is an automorphism of V of p-power order). Prove that there is some nonzero element $v \in V$ such that $\varphi(v) = v$, i.e. φ has a nonzero fixed point on V.

2.4. **Some extra questions.**

QUESTION 2.40. Let G be a group of order pqr where p, q and r are primes with $p < q < r$. Prove that a r-Sylow subgroup of G is normal.

QUESTION 2.41 (FALL 2015). Let G be a finite group with center $Z(G)$. Let $H \leq G$ be a subgroup with centralizer $C_G(H) = \{g \in G \mid ghg^{-1} = h \text{ for all } h \in H\}$.

(1) If p does not divide the order of $G/Z(G)$, the p does not divide the order of any conjugacy class in G.
(2) If p does not divide the size of any conjugacy class C, then $C_G(P) \cap C \neq \emptyset$ for any Sylow subgroup P of G.
(3) Using (2), prove the converse of (1).

QUESTION 2.42 (FALL 2017). Let G be a finitely generated group and let n be a positive integer. Prove:

(1) There are at most finitely many subgroups H of G such that $[G : H] = n$.
(2) For every subgroup H of G with finite index, there is a characteristic subgroup C of G contained in H with finite index.

(*Hint*. Since G is finitely generated, there are only finitely many group homomorphisms from G to the symmetric group S_n).

QUESTION 2.43 (FALL 2018). For any group G, define $\Phi(G)$, called called the *Frattini subgroup* of G, to be the intersection of all maximal subgroups of G. Prove that

(1) $\Phi(G)$ is a characteristic subgroup of G.
(2) If G is nilpotent, then all maximal subgroups of G are normal and have prime index. Conclude that the derived subgroup $[G, G]$ is contained in $\Phi(G)$.
(3) If G is finitely generated, then every proper subgroup H is contained in a maximal subgroup.

3. RINGS AND MODULES

QUESTION 3.1. Let R denote the ring of *Gaussian integers* $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$. Recall that R is a Euclidean domain (and hence a PID) with respect to the norm map $|\cdot| : R \to \mathbb{Z}$ defined by

$$|a + ib| = a^2 + b^2.$$

(1) Find the units in R.
(2) Recall a prime element π in R is an element such that the ideal (π) generated by π is a prime ideal. Show that $1 + i$ and 7 are prime ideals.
(3) Let p be a prime in $\mathbb{Z}$ and let $\pi \in R$ such that $|\pi| = p$. Show that π is prime in R. Moreover, show that such a prime p satisfies $p \equiv 1 \bmod 4$.

Remarks. FERMAT showed that every prime $p \equiv 1 \bmod 4$ is a norm of a Gaussian integer.

QUESTION 3.2. Let $\alpha = \sqrt{3}$ and let

$$R = \mathbb{Z}[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{Z}\}.$$

Denote P for the principal ideal of R generated by 5.

(1) Show that P is a prime ideal and R/P is a field with 25 elements.
(2) Prove that the ideal (11) generated by 11 is not a prime ideal of R.

DEFINITION 3.3. A ring R is said to be *Noetherian* if any ascending chain of ideals in R stabilizes, i.e. if

$$0 = I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots ,$$

then there is an integer $m \geq 0$ such that $I_m = I_{m+1}$.

QUESTION 3.4. Show that every principal ideal domain is Noetherian. (Do not use the fact that a ring is Noehterian if its ideals are finitely generated.)

QUESTION 3.5. Let R be a commutative ring with $1 \neq 0$ such that for every $x \in R$, there is a natural number $n > 1$ such that $x^n = x$. Show that every prime ideal of R is maximal.

QUESTION 3.6. Let E be a field, and $f, g \in E[X]$ be irreducible quadratic polynomials. Let

$$K = E[X]/(f) \quad \text{and} \quad L = E[X]/(g).$$

Show that

$$M := E[X, Y]/(f(X), g(Y))$$

is a field if and only if K and L are non-isomorphic as rings (or fields).

QUESTION 3.7 (SPRING 2020). Let A, B be commutative rings with 1. Show that any ideal of $A \times B$ is of the form $I \times J$ for ideals $I \leq A$ and $J \leq B$.

QUESTION 3.8 (SPRING 2020). Let R be the set of all polynomials over a field F whose linear coefficient is 0. (Make sure you see why R is a ring.)

(1) Determine $R^\times$, the units in R.
(2) Show that R is not a UFD. (*Hint.* both x^2 and x^3 are irreducible.)

QUESTION 3.9 (FALL 2021). Let R be a commutative ring and let M be a maximal ideal of R.

(1) If M is principal, show that there is no ideal $I \leq R$ satisfying $M^n \subsetneq I \subsetneq M^{n-1}$ for any $n \geq 1$.
(2) When M is not principal, give an example of an ideal I satisfying $M^n \subsetneq I \subsetneq M^{n-1}$ for any $n \geq 1$.

QUESTION 3.10 (FALL 2018). Let R be a commutative integral domain. A left R-module M is said to be *divisible* if for any $m \in M$, and nonzero $r \in R$, there is an $m' \in M$ such that $rm' = m$. In other words, $rM = M$ for any nonzero $r \in R$.

(1) Show that $\mathbb{Q}/\mathbb{Z}$ is a divisible $\mathbb{Z}$-module.
(2) Let R be a PID and not a field. Show that no nonzero finitely generated ideal of R is divisible.

QUESTION 3.11 (FALL 2023). Let $\Phi_{12}(x) = x^4 - x^2 + 1 \in \mathbb{Q}[x]$.

(1) Show that Φ_{12} is irreducible over $\mathbb{Q}$. (It is the minimal polynomial of a primitive 12-th root of unity.)
(2) Give an explicit matrix $A \in M_4(\mathbb{Q})$ with characteristic polynomial $\Phi_{12}(x)$.

QUESTION 3.12. Let R be a local ring with maximal ideal $\mathfrak{m}$. Let $A = \operatorname{diag}(\alpha_1, \ldots, \alpha_n)$ be an invertible matrix with $\alpha_i \neq \alpha_j \bmod \mathfrak{m}$ for any $i \neq j$. Show that the R-algebra generated by powers of A is the algebra of diagonal matrices.

QUESTION 3.13 (SPRING 2019). Let R be a commutative ring with 1 having pairwise distinct maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$ such that $\mathfrak{m}_1^{n_1} \cdots \mathfrak{m}_k^{n_k} = 0$.

(1) Show that
$$R \cong R/\mathfrak{m}_1^{n_1} \times \cdots \times R/\mathfrak{m}_k^{n_k}.$$
(2) Show that an element of R is either a unit or a nilpotent.
(3) Give an example of such an R.

QUESTION 3.14 (SPRING 2019). Let p be a prime and $d \geq 1$ be a positive integer. Determine the number of monic irreducible polynomials of degree d over $\mathbb{F}_p$.

QUESTION 3.15 (FALL 2018). A ring homomorphism $f : R \to S$ is called *centralizing* if the ring S is generated by $f(R)$ together with $C_S(f(R)) = \{s \in S \mid sf(r) = f(r)s \text{ for all } r \in R\}$. (For example, if f is surjective or if S is commutative, then f is evidently centralizing.) Prove:

(1) Composites of centralizing ring homomorphisms are centralizing.
(2) If f is centralizing, then $f(I)S$ is an ideal of S for every ideal I of R.

References

[DF04] David S. Dummit and Richard M. Foote, *Abstract algebra*, Wiley (2004), 1–946.