Math 721 Problem List (last updated on 2025-10-13)

1. If p is a prime number, prove that the nonzero elements of $\mathbb{Z}_p$ form a multiplicative group of order $p-1$. Show that this statement is false if p is not a prime.

2. (a) Prove that the relation given by $a \sim b \iff a - b \in \mathbb{Z}$ is an equivalence relation on the additive group $\mathbb{Q}$.
   (b) Prove that $\mathbb{Q}/\mathbb{Z}$ is an infinite abelian group.

3. Let p be a prime number and let $\mathbb{Z}(p^\infty)$ be the following subset of the group $\mathbb{Q}/\mathbb{Z}$:

$$\mathbb{Z}(p^\infty) = \{\overline{(a/b)} \in \mathbb{Q}/\mathbb{Z} \mid, a, b \in \mathbb{Z} \text{ and } b = p^i \text{ for some } i \geq 0\}$$

   Prove that $\mathbb{Z}(p^\infty)$ is an infinite subgroup of $\mathbb{Q}/\mathbb{Z}$.

4. If G is a finite group of even order, prove that G has an element of order two.

5. Let Q_8 be the multiplicative group generated by the complex matrices

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \text{ and } B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

   Observe that $A^4 = B^4 = I_2$ and $BA = AB^3$. Prove that Q_8 is a group of order 8.

6. Let G be a group and let $\mathrm{Aut}(G)$ denote the set of all automorphisms of G.

   (a) Prove that $\mathrm{Aut}(G)$ is a group with composition of functions as binary operation.
   (b) Prove that $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$, $\mathrm{Aut}(\mathbb{Z}_6) \cong \mathbb{Z}_2$, $\mathrm{Aut}(\mathbb{Z}_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$ (p prime)

7. Let G be an infinite group that is isomorphic to each of its proper subgroups. Prove that $G \cong \mathbb{Z}$.

8. Let G be the multiplicative group of 2×2 invertible matrices with rational entries. Show that

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \text{ and } B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$$

   have finite orders but AB has infinite order.

9. Let G be an abelian group containing elements a and b of orders m and n, respectively. Prove that G contains an element of order $\mathrm{lcm}(m, n)$.

10. Let H, K be subgroups of a group G. Prove that HK is a subgroup of G if and only if $HK = KH$.

11. Let H, K be subgroups of finite index of a group G such that $[G : H]$ and $[G : K]$ are relatively prime. Prove that $G = HK$.

12. Let H, K, N be subgroups of G such that $H \subseteq N$. Prove that $HK \cap N = H(K \cap N)$.
13. Let H, K, N be subgroups of G such that $H \subseteq K, H \cap N = K \cap N$ and $HN = KN$. Prove that $H = K$.
14. Let H be a subgroup of G. For $a \in G$, prove that aHa^{-1} is a subgroup of G that is isomorphic to H.
15. Let G be a finite group and H a subgroup of G of order n. If H is the only subgroup of G of order n, prove that H is normal in G.
16. If H is a cyclic normal subgroup of a group G, then every subgroup of H is normal in G.
17. What is $Z(S_n)$ for $n \geq 2$?
18. If H is a normal subgroup of G such that H and G/H are finitely generated, then G is finitely generated.
19. If N is a normal subgroup of G, $[G : N]$ is finite, H is a subgroup of G, $|H|$ is finite, and $[G : N]$ and $|H|$ are relatively prime, then H is a subgroup of N.
20. If N is a normal subgroup of G, $|N|$ is finite, H is a subgroup of G, $[G : H]$ is finite, and and $[G : H]$ and $|N|$ are relatively prime, then N is a subgroup of H.
21. If G is a finite group and H, K are subgroups of G, then
$$[G : H \cap K] \leq [G : H][G : K]$$
22. If H, K, L are subgroups of a finite group G such that $H \subseteq K$, then
$$[K : H] \geq [L \cap K : L \cap H]$$
23. Let H, K be subgroups of a group G. Assume that $H \cup K$ is a subgroup of G. Prove that either $H \subseteq K$ or $K \subseteq H$.
24. Let G be an abelian group, H a subgroup of G such that G/H is an infinite cyclic group. Prove that $G \cong H \times G/H$.
25. Let P be a Sylow p-subgroup of a finite group G. Prove that $N(N(P)) = N(P)$.
26. If H is a subgroup of G, prove that the group $N(H)/C(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.
27. If $G/Z(G)$ is cyclic, then G is abelian.
28. Every group of order 28, 56, 200 must contain a normal Sylow subgroup, and hence is not simple.
29. There is no simple group of order 30.

30. There is no simple group of order 24.

31. There is no simple group of order 36.

32. There is no simple group of order 48.

33. There is no simple group of order 56.

34. There is no simple group of order 148.

35. Let G be a group of order p^2q where p, q are distinct primes. Show that G is not simple.

36. If every Sylow p-subgroup of a finite group G is normal for every prime p, then G is isomorphic to the direct product of its Sylow subgroups.

37. If P is a normal Sylow p-subgroup of a finite group G and $f : G \to G$ is a group homomorphism, then $f(P) \subseteq P$.

38. Let G be a cyclic group of order n. Let d be a divisor of n. Prove that G has a unique subgroup with d elements.

39. A semidirect product $H \rtimes_\varphi K$ is unchanged up to isomorphism if the action $\varphi : K \to \mathrm{Aut}(H)$ is composed with an automorphism of K. More precisely, for automorphisms $f : K \to K$, prove that $H \rtimes_{\varphi \circ f} K \cong H \rtimes_\varphi K$.

40. Prove that an abelian group has a composition series if and only if it is finite.

41. Prove that a solvable simple group is abelian.

42. Prove that a solvable group that has a composition series is finite.

43. If G is a finite group and H is a normal subgroup of G, prove that G has a composition series where one of its terms is H.

44. Let G be a solvable group and H a nontrivial normal subgroup of G. Prove that G has a nontrivial normal subgroup A such that A is contained in H and A is abelian.

45. If $K \subseteq F$ is a field extension, $u, v \in F$, v is algebraic over $K(u)$ and v is transcendental over K, then u is algebraic over $K(v)$.

46. If $K \subseteq F$ is a field extension and $u \in F$ is algebraic of odd degre over K, then so is u^2 and $K(u) = K(u^2)$.

47. Let $K \subseteq F$ be a field extension. If $X^n - a \in K[X]$ is irreducible and $u \in F$ is a root of $X^n - a$ and m divides n, then the degree of u^m over K is n/m. What is the irreducible polynomial of u^m over K?

48. Let $K \subseteq R \subseteq F$ be an extension of rings with K, F fields. If $K \subseteq F$ is algebraic, prove that R is a field.

49. Let $f = X^3 - 6X^2 + 9X + 3 \in \mathbb{Q}[X]$.

(a) Prove that f is irreducible in $\mathbb{Q}[X]$.

(b) Let u be a real root of f. Consider the extension $\mathbb{Q} \subseteq \mathbb{Q}(u)$. Express each of the following elements in terms of the basis $\{1, u, u^2\}$ of the $\mathbb{Q}$-vector space $\mathbb{Q}(u)$: $u^4; u^5; 3u^5 - u^4 + 2; (u+1)^{-1}; (u^2 - 6u + 8)^{-1}$.

50. Let $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Find $[F : \mathbb{Q}]$ and a basis of F over $\mathbb{Q}$.

51. Let K be a field. In the field $K(X)$, let $u = X^3/(X+1)$. What is $[K(X) : K(u)]$?

52. Let $K \subseteq F$ be a field extension. If $u, v \in F$ are algebraic over K of degrees m and n, respectively, then $[K(u, v) : K] \leq mn$. If m and n are relatively prime, then $[K(u, v) : K] = mn$.

53. Let $K \subseteq F$ be a field extension. Prove that F is algebraic over K if and only if for every intermediary field $K \subseteq E \subseteq F$, every K-embedding $\sigma : E \to E$ is an isomorphism.