1. Let $\mathbf{H}$ be a subgroup of the group $\mathbf{G}$.
   (a) Define the set $\mathbf{G}/\mathbf{H}$ of (left) cosets of $\mathbf{H}$ in $\mathbf{G}$.
   (b) State and prove for finite groups *Lagrange's Theorem*.
   (c) Let $\mathbf{G}$ be a finite group with n elements. Prove that $x^n = e$ holds for every $x \in \mathbf{G}$.

2. Let $\mathbf{G}$ be a group. For any two elements $x, y \in \mathbf{G}$, the element $x^{-1}y^{-1}xy$ is called a *commutator*. The subgroup of $\mathbf{G}$ which is generated by all commutators is called the *commutator subgroup* $\mathbf{G}'$.
   (a) Prove that the inverse of a commutator is a commutator and that $\mathbf{G}'$ consists of finite products of commutators.
   (b) Prove that the group $\mathbf{G}'$ is normal in $\mathbf{G}$ and that the factor group $\mathbf{G}/\mathbf{G}'$ is abelian.
   (c) Let $\mathbf{H}$ be a normal subgroup of $\mathbf{G}$ such that the factor group $\mathbf{G}/\mathbf{H}$ is abelian. Prove that $\mathbf{G}' \subseteq \mathbf{H}$.

3. (a) A subgroup H of a group G is called *characteristic* if $\varphi(H) = H$ for any automorphism φ of G. Show that a characteristic subgroup is normal.
   (b) Suppose that $G = HK$, where H and K are characteristic subgroups of G with $H \cap K = \{e\}$. Prove that $\mathrm{Aut}(G) \cong \mathrm{Aut}(H) \times \mathrm{Aut}(K)$. (Here, $\mathrm{Aut}(\cdot)$ denotes the group of automorphisms.)

4. (a) Let H, K be groups. Give a definition of what it means for G to be a semi-direct product of H, K.
   (b) Give an example of a group structure on the set $\mathbb{Z}_2 \times \mathbb{Z}_5$ which is different from the product group structure. Prove that the structure you describe is actually different.
   (c) Let H and K be groups. Let $\varphi : K \to \mathrm{Aut}(H)$ be a homomorphism. Let $\sigma : K \to K$ be an automorphism of K. Let $\psi = \varphi \circ \sigma$. Prove that the semi-direct products $H \rtimes_\varphi K$ and $H \rtimes_\psi K$ are isomorphic.

5. Let $(\mathbf{A}, +)$ be a commutative group and $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n$ be subgroups of $\mathbf{A}$. Define:
   (a) $\mathbf{A}$ is the sum of the subgroups $\mathbf{A}_i$.
   (b) $\mathbf{A}$ is the internal *direct* sum of the $\mathbf{A}_i$.
   (c) What do finite abelian groups look like that are *not* the direct sum of non-trivial subgroups?

6. (a) State the structure theorem for finite abelian groups.
   (b) List up to isomorphism classes all abelian groups of order 100, e.g., in terms of direct sums of cyclic groups.

7. Let $(\mathbf{V}, T)$ be a pair consisting of a finite dimensional vector space $\mathbf{V}$ over a field $\mathbf{F}$ and a linear map T on $\mathbf{V}$. How does $\mathbf{V}$ become an $\mathbf{F}[x]$-module?

8. Let $\mathbf{M}$ be a module over the p.i.d. $\mathbf{D}$ and let $d \in \mathbf{D}$. Define: $\mathbf{M}(d) = \{x \mid d.x = 0\}$. Prove that if $(d_1, d_2) = (1)$ and $d_1 \cdot d_2 = d$, then $\mathbf{M}(d) = \mathbf{M}(d_1) \oplus \mathbf{M}(d_2)$.

9. (a) Define: $\mathbf{N}$ is a normal subgroup of $\mathbf{G}$.
   (b) Define for a normal subgroup $\mathbf{N}$ the factor group $\mathbf{G}/\mathbf{N}$.
   (c) Explain that a homomorphic image of a group is isomorphic to a factor group.

10. (a) State the Sylow Theorems.
    (b) Let H be a normal subgroup of order p^k of a finite group G. Prove that H is contained in every p-Sylow subgroup of G.

11. (a) Assume without proof that the polynomial $p(x) = x^4 + 6x + 3$ is irreducible. Let ϑ be a root of $p(x)$. Determine $(2 + \vartheta)^{-1}$ in the field $\mathbb{Q}(\vartheta)$.
    (b) Let K/F be a finite field extension. Define what it means for this extension to be Galois. Define the Galois group of a Galois extension.

(c) Let K/F be a Galois extension with Galois group $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Find the number of subfields of K that have degree 4 over F. Justify your answer carefully.

12. Let F be a finite field of characteristic $p > 0$. Let $\varphi : F \to F$, $a \mapsto a^p$. Prove that φ is a field automorphism.

13. (a) Define that $T : \mathbf{V} \to \mathbf{V}$ is a linear map on the vector space $\mathbf{V}$ over the field $\mathbf{F}$.
    (b) Define that $\mathbf{A}$ is the matrix for T with respect to the basis $e_1, \ldots, e_n$.
    (c) Let $\mathbf{A}$ be an $n \times n$ matrix with entries from the field $\mathbf{F}$. Show that there is a polynomial $p(x) \in \mathbf{F}[x]$ such that $p(\mathbf{A}) = 0$.

14. (a) Let $\mathcal{A}$ be an abstract class (that is closed under isomorphic copies) of algebras. Let $q_i : A_i \to A$ be a co-terminal family of homomorphisms. Define that A is a sum system.
    (b) Prove that the class $\mathcal{A}$ of modules over a ring A admits sums.
    (c) Define that the module $\mathbf{M}$ is the internal direct sum $\mathbf{M} = \mathbf{M}_1 \oplus \mathbf{M}_2$.

15. (a) Let X be any set and let $\mathcal{A}$ be an abstract class of algebras. State the definition of: the algebra $F_{\mathcal{A}}(X)$ is the free $\mathcal{A}$ algebra, freely generated by X.
    (b) Let $\mathcal{V}$ be the class of vector spaces over a field F. Prove that every vector space is freely generated by some set B.

16. (a) List all subgroups of the additive group $\mathbb{Z}$ of integers.
    (b) Prove your answer for part (a).

17. Let a and b be elements of a principal ideal domain $\mathbf{D}$.
    (a) Define: d is the greatest common divisor of a and b.
    (b) Prove that $\{xa + yb \mid x, y \in \mathbf{D}\}$ is the smallest ideal in $\mathbf{D}$ which contains a and b.
    (c) Prove that the greatest common divisor of a and b exists and that it is of the form $xa + yb$ for certain x and y in $\mathbf{D}$.

18. (a) Let G be a group. For any subgroup H of G and nonempty subset $A \subset G$, define $N_H(A)$ to be the set $\{h \in H \mid hAh^{-1} = A\}$. Prove that $N_H(A) = N_G(A) \cap H$.
    (b) Let G be a group and H a subgroup of G. Give the definition of the center $Z(G)$ and the centralizer $C_G(H)$.
    (c) Let G be a group and H a subgroup of G of order 2. Prove that $N_G(H) = C_G(H)$. Deduce that if $N_G(H) = G$, then H is contained in $Z(G)$.

19. (a) Assume without proof that the polynomial $p(x) = x^4 + 6x + 3$ is irreducible. Let ϑ be a root of $p(x)$. Determine ϑ^{-1} in the field $\mathbb{Q}(\vartheta)$.
    (b) Determine the splitting field and degree over $\mathbb{Q}$ of
        i. $x^4 - 1$,
        ii. $x^2 - 2$,
        iii. $x^4 + 1$.
    (c) Among the above three splitting fields, are there two which are isomorphic? Prove your answer.

20. (a) Define cyclic groups.
    (b) Prove that a homomorphic image of a cyclic group is cyclic.
    (c) Prove that a subgroup of a cyclic group is cyclic.
    (d) Prove that every cyclic group is a homomorphic image of the additive group $\mathbb{Z}$ of integers.

21. Prove that the multiplicative group of a finite field is cyclic.

22. Let $p(x)$ be an irreducible polynomial over the field $\mathbf{F}$.
    (a) Explain why the factor ring $\mathbf{E} = \mathbf{F}[x]/(p(x))$ is a field.
    (b) Prove that $a \mapsto a + (p(x))$ is an embedding of $\mathbf{F}$ into $\mathbf{E}$; thus $\mathbf{E}$ can be perceived as an extension of $\mathbf{F}$.
    (c) Prove that $p(x)$ has a root in $\mathbf{E}$.
    (d) Let $\mathbf{F} = \mathbb{Q}$ be the field of rational numbers and $p(x) = x^2 - 2$. What do elements of $\mathbb{Q}[x]/(x^2 - 2)$ look like?

23. Prove that every vector space over a field F has a basis S and that every vector space is free for the class $\mathcal{F}$ of all vector spaces over F.

24. Let $\mathcal{D}$ be the class of modules over the principal ideal domain (p.i.d.) D. Let $\mathbf{M}$ be a free D-module with finite base S. Prove that any other base of $\mathbf{M}$ has the same number of elements. (Hint: Take a prime element p of D and show that $\mathbf{M}/p\mathbf{M}$ can be made into a vector space.)

25. Let $(G, *, ^{-1}, e)$ be a finite group of order n.
    (a) Let H be a subgroup of G where $|H| = m$. Prove that m divides n.
    (b) Let $x \in G$. Prove that $x^n = e$.

26. (a) State the primary decomposition theorem for finitely generated torsion modules.
    (b) How does this theorem relate to the decomposition of a vector space $\mathbf{V}$ over the field $\mathbb{C}$ of complex numbers into generalized eigenspaces for a linear map T on $\mathbf{V}$?
    (c) List all isomorphism classes of abelian groups of order 144.

27. Let $\mathcal{A}$ be the class of fields of a fixed characteristic. Prove that for $X \neq \emptyset$, the class $\mathcal{A}$ does not admit free algebras. What can you say for $X = \emptyset$?

28. (a) Let R be a ring. Define what it means for R to be an integral domain.
    (b) Let R be an integral domain. Let $p \in R$. Give the definitions of what it means for p to be *irreducible* and of what it means for p to be *prime*. Prove that *prime* implies *irreducible*. Prove that the converse of this statement is false. Give a sufficient condition under which the converse does hold, and prove your statement.

29. (a) Consider the polynomial $f(x) := x^8 - x \in \mathbb{F}_2[x]$, where $\mathbb{F}_2$ is the field with two elements. Prove that the set K of all roots of f (in an algebraic closure of $\mathbb{F}_2$) forms a field. How many elements does this field have?
    (b) What is the prime subfield F of K?
    (c) Is K a Galois extension of F? Justify your answer carefully.

30. (a) Let N be a subgroup of G. Give a definition of what it means for N to be normal.
    (b) Let N be a normal subgroup of the finite group G. Assume that the order of N and the index of N are relatively prime. Prove that N is the unique subgroup of G of order $\#N$. (It is allowed to cite a theorem from class, but you must state the theorem correctly and in its entirety.)
    (c) Let H, K be subgroups of a group. Prove that HK is a subgroup if and only if $HK = KH$.

31. (a) Give the definition of what it means for a polynomial $f(x) \in F[x]$ over a field F to be separable.
    (b) Let $D_x f(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$ be the derivative of $f = \sum_{i=0}^{n} a_i x_i \in F[x]$. Prove that f is separable if and only if f and $D_x f$ are relatively prime.

32. Let $\mathbf{G}$ and $\mathbf{H}$ be groups and $\varphi : \mathbf{G} \to \mathbf{H}$ be a surjective homomorphism. Define the factor group $\mathbf{G}/\ker\varphi$, and prove that $\mathbf{G}/\ker\varphi \cong \mathbf{H}$.

33. (a) Prove that the characteristic of a finite field $\mathbf{F}$ is a prime.
    (b) Prove that the number of elements of a finite field is p^n for some prime p and natural number $n \geq 1$.

34. (a) Let $T : V \to V$ be a linear map on a vector space V over a field F. State for T the decomposition theorem according to the elementary divisors, which assumes that $p(x) = p_1(x)^{n_1} \cdots p_k(x)^{n_k}$ is the prime factorization of the minimal polynomial for T.
    (b) What are the possible elementary divisors of a linear map T on $\mathbb{R}^4$ if the minimal polynomial for T is $p_T(x) = (x-1)^2(x+1)$?

35. Assume that the characteristic polynomial for a linear map T on $\mathbb{R}^3$ is $c_T(x) = (x-1)(x+1)^2$.
    (a) Find the minimal polynomial for T in the case that T is cyclic.
    (b) Find the minimal polynomial for T in the case that T has an eigenbase.

36. Assume that the characteristic polynomial for a linear map T on $\mathbb{R}^4$ is $c_T(x) = (x+1)^4$.
    (a) Find a matrix A for T for which $A^4 = 0$.
    (b) Find all similarity classes of maps, say according to elementary divisors or Jordan normal forms, which have $(x+1)^4$ as their characteristic polynomial.

37. (a) Prove that the class $\mathcal{A}$ of modules over a commutative ring A admits sums.
    (b) Let $\mathcal{F}$ be the class of fields of characteristic zero. Prove that $\mathcal{F}$ does not have sums.

38. (a) Prove that the class of modules over a commutative ring A admits for every set B a free module over A. What does it look like?
    (b) Explain why, in the case that A is a field, every module over A is free.
    (c) Prove that the class $\mathcal{F}$ of fields of characteristic zero does not have free objects for X different from the empty set.
    (d) What is the free field of characteristic zero over the empty set?

39. (a) Define that $\mathbf{P}$ is a projective module over the ring A.
    (b) Prove that free modules over A are projective.

40. Let $\mathbf{M}$ be a module over the principal ideal domain D and let $x \in \mathbf{M}$. How is the period $\operatorname{per}(x)$ of x defined? What is $\operatorname{per}(0)$?

41. Let $\mathbf{M}$ be a module over the p.i.d. $\mathbf{D}$, and let $d \in \mathbf{D}$. Define: $\mathbf{M}(d) = \{x \in \mathbf{M} \mid d.x = 0\}$. Prove that if $(d_1, d_2) = (1)$ and $d_1 \cdot d_2 = d$, then $\mathbf{M}(d) = \mathbf{M}(d_1) \oplus \mathbf{M}(d_2)$.

42. (a) State the primary decomposition theorem for finitely generated torsion modules over a principal ideal domain.
    (b) What does this theorem say for finite abelian groups?
    (c) How does this theorem relate to the decomposition of a vector space $\mathbf{V}$ over the field $\mathbb{C}$ of complex numbers into generalized eigenspaces for a linear map T on $\mathbf{V}$?

43. Let A be a commutative ring where $1 \neq 0$. Let M be a maximal ideal. Prove that the quotient ring A/M is a field.

44. Let $\mathcal{A}$ be an abstract class of algebras (that is, $\mathcal{A}$ is closed under isomorphic copies). Let $p_i : A \to A_i$ be a co-initial family of homomorphisms. Define that $p_i : A \to A_i$ is a product system in $\mathcal{A}$.

45. Define that the module $\mathbf{M}$ is the internal direct sum of $\mathbf{M}_1$ and $\mathbf{M}_2$: $\mathbf{M} = \mathbf{M}_1 \oplus \mathbf{M}_2$.

46. Let $(\mathbf{V}, T)$ be a pair consisting of a finite-dimensional vector space $\mathbf{V}$ over a field F and a linear map T on $\mathbf{V}$. How does $\mathbf{V}$ become an $F[x]$-module?

47. (a) Find an $n \times n$ matrix A such that $A^n = 0$, but $A^{n-1} \neq 0$.
    (b) Let $p(x) = a_0 + a_1 x + \cdots + x^n$ be any polynomial of degree n. Prove that there is an $n \times n$ matrix A such that $p(x)$ is the characteristic polynomial. (Hint: Define a cyclic space (F^n, T), where $T(e_1) = e_2$, $T(e_2) = e_3$, …, $T(e_{n-1}) = e_n$, and $T(e_n) = -a_0.e_1 - a_1.e_2 - \cdots - a_{n-1}.e_n$.)
    (c) Find all Jordan forms of 4×4 matrices where the characteristic polynomial is x^4.

48. Let $\mathcal{A}$ be an abstract class of similar algebras. Let X be any set. Define that $\mathbf{F}_{\mathcal{A}}(X)$ is the free $\mathcal{A}$-algebra, freely generated by X.

49. State Zorn's lemma.

50. Prove that every vector space over a field F is free.

51. (a) State one version of the structure theorem for finite abelian groups.
    (b) List up to isomorphism classes all abelian groups of order 200, e.g. in terms of direct sums of cyclic groups.

52. Let $|G| = p^n q$ with $p > q$ prime. Prove that G contains a unique normal subgroup of order p^n.

53. Assume that the characteristic polynomial for the linear map T on $\mathbb{R}^3$ is $c_T(x) = (x-1)(x+1)^3$.
    (a) Find the minimal polynomial for T in the case that T is cyclic.
    (b) Find the minimal polynomial for T in the case that T is symmetric.

54. Let $T : V \to V$ be a linear map on a vector space V over a field F.
    (a) Define: $m_T(x)$ is the minimal polynomial of T.
    (b) Define: $c_T(x)$ is the characteristic polynomial of T.
    (c) State the *Cayley-Hamilton theorem.*
    (d) What can you say about the minimal polynomial of a diagonalizable linear map?
    (e) Let $T : \mathbb{R}^3 \to \mathbb{R}^3$ be a linear map with characteristic polynomial $c_T(x) = x^2(x-1)$. Find the possible Jordan forms of matrices for T.

55. (a) Let G be a group and $x \in G$ an element of finite order n. Prove that if n is odd, then $x^k \neq x^{-k}$ for all $k = 1, 2, \ldots, n-1$.
    (b) Let G be a finite group. Let H be a subgroup of G and let $N \triangleleft G$ be a normal subgroup. Prove that if $\gcd(\#H, |G : N|) = 1$, then H is a subgroup of N.

56. (a) As detailed as you can, state Sylow's theorem.
    (b) A group G is called *simple* if it has no non-trivial normal subgroups. Prove that there are no simple groups of order 124.
    (c) Determine explicitly the set of 3-Sylow subgroups of the symmetric group S_4. Hint: use Sylow's theorem and additional explicit considerations.
    (d) For each isomorphism class of abelian groups of order 252, give one representative.

57. (a) Find the degree of the field extension $\mathbb{Q}(\sqrt{2} + \sqrt{3})/\mathbb{Q}$. Justify your answer in full detail.
    (b) Find the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$.
    (c) Is $\mathbb{Q}(\sqrt{2} + \sqrt{3})/\mathbb{Q}$ a Galois extension? Determine $\mathrm{Aut}(\mathbb{Q}(\sqrt{2} + \sqrt{3})/\mathbb{Q})$ explicitly.

58. (a) Let k be an infinite field, endowed with the Zariski topology. Is the Zariski topology on the product $k \times k$ the same as the product topology? Prove your answer.
    (b) As detailed as you can, state Hilbert's Nullstellensatz.

59. (a) Let R, S be rings and $\varphi : R \to S$ a ring homomorphism. If I is an ideal of R, prove that $\varphi(\operatorname{rad} I) \subseteq \operatorname{rad}(\varphi(I))$. If in addition φ is surjective and I contains the kernel of φ, prove that $\varphi(\operatorname{rad} I) = \operatorname{rad}(\varphi(I))$.

    (b) Let k be a field and $I := (f_1, \ldots, f_m) \subset k[x_1, \ldots, x_n]$ an ideal. Let $g \in \mathcal{I}(\mathcal{Z}(I))$. Prove the following: if we take $f_1, \ldots, f_m$ to be elements of $k[x_1, \ldots, x_{n+1}]$, then $\mathcal{Z}((f_1, \ldots, f_m, x_{n+1}g - 1)) = \emptyset$.

60. (a) Define what it means for a set G to be a group. Define what it means for a subset H of G to be a subgroup.

    (b) Let G be a finite group. Prove that G cannot have a subgroup H with $\#H = n - 1$, where $n = \#G > 2$. (Give a direct proof—you must NOT cite any theorems from class.)

61. (a) As detailed as you can, state Sylow's theorem.

    (b) The proof given in class was based on a theorem called "The Class Equation." State "The Class Equation" as best you can.

    (c) Prove that a group of order 30 contains a normal subgroup.

62. (a) Let K/F be a finite field extension. Define what it means for this extension to be Galois. Define the Galois group of a Galois extension.

    (b) Which of the following extensions over $\mathbb{Q}$ are Galois? (Justify your answer carefully.)

        i. $\mathbb{Q}(\sqrt{5})$,

        ii. $\mathbb{Q}(\sqrt[3]{5})$,

        iii. $\mathbb{Q}(\sqrt{5}, \sqrt{2})$.

    (c) Let K/F be a Galois extension with Galois group $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Find the number of subfields of K that have degree 4 over F. Justify your answer carefully.

63. (a) Let I, J be ideals in the ring R. Prove that $\operatorname{rad}(IJ) = \operatorname{rad} I \cap \operatorname{rad} J$.

    (b) Let $V = \mathcal{Z}(x^2 - y) \subset \mathbb{A}^2$. Prove that $\mathbb{A}^1$ is isomorphic to V by providing an explicit isomorphism $\varphi : \mathbb{A}^1 \to V$. Provide also the associated k-algebra isomorphism $\tilde{\varphi} : k[V] \to k[\mathbb{A}^1]$. Finally, provide the inverses of φ and $\tilde{\varphi}$.

    (c) Let k be an algebraically closed field. Use Hilbert's Nullstellensatz to prove that every proper radical ideal in $k[x_1, \ldots, x_n]$ is the intersection of maximal ideals.

64. Define cyclic groups and prove that every cyclic group is a homomorphic image of $\mathbb{Z}$. Prove that cyclic groups are either isomorphic to $\mathbb{Z}$ or isomorphic to the integers modulo n for some $n > 0$.

65. (a) Let X be any set. Define that $\mathbf{F}_{\mathcal{G}}(X)$ is the free group freely generated by the set X.

    (b) Describe $\mathbf{F}_{\mathcal{G}}(\emptyset)$ and $\mathbf{F}_{\mathcal{G}}(1)$.

66. (a) State the structure theorem for finitely generated abelian groups.

    (b) List up to isomorphism classes all abelian groups of order 144, e.g. in terms of direct sums of cyclic groups.

67. (a) Define that I is an ideal of a ring $\mathbf{A}$ (with unit) and state the homomorphism theorem for rings.

    (b) Explain how the ideals J that contain I correspond to the ideals of $\mathbf{A}/I$.

    (c) Define that M is a maximal ideal. Prove that the factor ring $\mathbf{A}/M$ is a field in the case that $\mathbf{A}$ is a commutative ring (with unit) and M a maximal ideal.

    (d) Prove that every commutative ring with unit admits a homomorphic image which is a field.

68. Let (V, T) be a pair consisting of a finite-dimensional vector space V over the field F and a linear map $T : V \to V$. Assign to the pair (V, T) a module over the polynomial ring $F[x]$.

69. Prove the following theorem:

    Let $T : \mathbf{V} \to \mathbf{V}$ be a linear map on a vector space $\mathbf{V}$. Then $\mathbf{V} = \mathbf{V}_1 \oplus \mathbf{V}_2$, where $\mathbf{V}_1$ and $\mathbf{V}_2$ are invariant under T and where T restricted to $\mathbf{V}_1$ is one-to-one and T restricted to $\mathbf{V}_2$ is nilpotent, that is, $T^k = 0$ for some k.

70. (a) State the fundamental theorem for finitely generated abelian groups.

    (b) List all abelian groups of order 100 according to elementary divisors or invariant factors.

    (c) For which numbers n is there exactly one abelian group of that order?

71. Find a 3×3 matrix $\mathbf{A}$ such that $\mathbf{A}^3 - 2\mathbf{A}^2 + 4\mathbf{A} = \mathrm{Id}$.

72. Let $T : \mathbb{R}^4 \to \mathbb{R}^4$ be a linear map whose characteristic polynomial is $c_T(x) = (x-1)^2(x-2)^2$. What are the possible Jordan normal forms for the matrix of T?