Title

D. Zack Garza

Friday 15th May, 2020

Contents

1 Question 1

Let G be a finite group with n distinct conjugacy classes. Let $g_1 \cdots g_n$ be representatives of the conjugacy classes of G.

Prove that if $g_i g_j = g_j g_i$ for all i, j then G is abelian.

2 Question 2

Let G be a group of order 105 and let P, Q, R be Sylow 3, 5, 7 subgroups respectively.

(a) Prove that at least one of Q and R is normal in G.

(b) Prove that G has a cyclic subgroup of order 35.

(c) Prove that both Q and R are normal in G.

(d) Prove that if P is normal in G then G is cyclic.

3 Question 3

Let R be a ring with the property that for every $a \in R, a^2 = a$.

(a) Prove that R has characteristic 2.

(b) Prove that R is commutative.

4 Question 4

Let F be a finite field with q elements.

Let n be a positive integer relatively prime to q and let ω be a primitive nth root of unity in an extension field of F.

Let $E = F[\omega]$ and let $k = [E : F]$.

(a) Prove that n divides $q^k - 1$.

(b) Let m be the order of q in $\mathbb{Z}/n\mathbb{Z}$. Prove that m divides k.

(c) Prove that $m = k$.

5 Question 5

Let R be a ring and M an R-module.

> Recall that the set of torsion elements in M is defined by
>
> $$\mathrm{Tor}(m) = \{m \in M \mid \exists r \in R,\ r \neq 0,\ rm = 0\}.$$

(a) Prove that if R is an integral domain, then $\mathrm{Tor}(M)$ is a submodule of M .

(b) Give an example where $\mathrm{Tor}(M)$ is not a submodule of M.

(c) If R has zero-divisors, prove that every non-zero R-module has non-zero torsion elements.

6 Question 6

Let R be a commutative ring with multiplicative identity. Assume Zorn's Lemma.

(a) Show that

$$N = \{r \in R \mid r^n = 0 \text{ for some } n > 0\}$$

is an ideal which is contained in any prime ideal.

(b) Let r be an element of R not in N. Let S be the collection of all proper ideals of R not containing any positive power of r. Use Zorn's Lemma to prove that there is a prime ideal in S.

(c) Suppose that R has exactly one prime ideal P . Prove that every element r of R is either nilpotent or a unit.

7 Question 7

Let ζ_n denote a primitive nth root of $1 \in \mathbb{Q}$. You may assume the roots of the minimal polynomial $p_n(x)$ of ζ_n are exactly the primitive nth roots of 1.

Show that the field extension $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is Galois and prove its Galois group is $(\mathbb{Z}/n\mathbb{Z})^\times$.

How many subfields are there of $\mathbb{Q}(\zeta_{20})$?

8 Question 8

Let $\{e_1, \cdots, e_n\}$ be a basis of a real vector space V and let

$$\Lambda := \left\{ \sum r_i e_i \,\middle|\, ri \in \mathbb{Z} \right\}$$

Let $\cdot$ be a non-degenerate ($v \cdot w = 0$ for all $w \in V \iff v = 0$) symmetric bilinear form on V such that the Gram matrix $M = (e_i \cdot e_j)$ has integer entries.

Define the dual of Λ to be

$$\Lambda^\vee := \{v \in V \mid v \cdot x \in \mathbb{Z} \text{ for all } x \in \Lambda\}.$$

(a) Show that $\Lambda \subset \Lambda^\vee$.

(b) Prove that $\det M \neq 0$ and that the rows of M^{-1} span $\Lambda^\vee$.

(c) Prove that $\det M = |\Lambda^\vee/\Lambda|$.

9 Question 9

Let A be a square matrix over the complex numbers. Suppose that A is nonsingular and that A^{2019} is diagonalizable over $\mathbb{C}$.

Show that A is also diagonalizable over $\mathbb{C}$.

10 Question 10

Let $F = \mathbb{F}_p$, where p is a prime number.

(a) Show that if $\pi(x) \in F[x]$ is irreducible of degree d, then $\pi(x)$ divides $x^{p^d} - x$.

(b) Show that if $\pi(x) \in F[x]$ is an irreducible polynomial that divides $x^{p^n} - x$, then $\deg \pi(x)$ divides n.

11 Question 11

How many isomorphism classes are there of groups of order 45?

Describe a representative from each class.

12 Question 12

For a finite group G, let $c(G)$ denote the number of conjugacy classes of G.

(a) Prove that if two elements of G are chosen uniformly at random,then the probability they commute is precisely

$$\frac{c(G)}{|G|}.$$

(b) State the class equation for a finite group.

(c) Using the class equation (or otherwise) show that the probability in part (a) is at most

$$\frac{1}{2} + \frac{1}{2[G : Z(G)]}.$$

Here, as usual, $Z(G)$ denotes the center of G.

13 Question 13

Let R be an integral domain. Recall that if M is an R-module, the *rank* of M is defined to be the maximum number of R-linearly independent elements of M .

(a) Prove that for any R-module M, the rank of $\mathrm{Tor}(M)$ is 0.

(b) Prove that the rank of M is equal to the rank of of $M/\mathrm{Tor}(M)$.

(c) Suppose that M is a non-principal ideal of R.

(d) Prove that M is torsion-free of rank 1 but not free.

14 Question 14

Let R be a commutative ring with 1.

Recall that $x \in R$ is nilpotent iff $xn = 0$ for some positive integer n.

(a) Show that every proper ideal of R is contained within a maximal ideal.

(b) Let $J(R)$ denote the intersection of all maximal ideals of R.

Show that $x \in J(R) \iff 1 + rx$ is a unit for all $r \in R$.

(c) Suppose now that R is finite. Show that in this case $J(R)$ consists precisely of the nilpotent elements in R.

15 Question 15

Let p be a prime number. Let A be a $p \times p$ matrix over a field F with 1 in all entries except 0 on the main diagonal.

Determine the Jordan canonical form (JCF) of A

(a) When $F = \mathbb{Q}$,

(b) When $F = \mathbb{F}_p$.

Hint: In both cases, all eigenvalues lie in the ground field. In each case find a matrix P such that $P^{-1}AP$ is in JCF.

16 Question 16

Let $\zeta = e^{2\pi i/8}$.

(a) What is the degree of $\mathbb{Q}(\zeta)/\mathbb{Q}$?

(b) How many quadratic subfields of $\mathbb{Q}(\zeta)$ are there?

(c) What is the degree of $\mathbb{Q}(\zeta, \sqrt[4]{2})$ over $\mathbb{Q}$?

17 Question 17

Let G be a finite group whose order is divisible by a prime number p. Let P be a normal p-subgroup of G (so $|P| = p^c$ for some c).

(a) Show that P is contained in every Sylow p-subgroup of G.

(b) Let M be a maximal proper subgroup of G. Show that either $P \subseteq M$ or $|G/M| = p^b$ for some $b \leq c$.

18 Question 18

(a) Suppose the group G acts on the set X . Show that the stabilizers of elements in the same orbit are conjugate.

(b) Let G be a finite group and let H be a proper subgroup. Show that the union of the conjugates of H is strictly smaller than G, i.e.

$$\bigcup_{g \in G} gHg^{-1} \subsetneq G$$

(c) Suppose G is a finite group acting transitively on a set S with at least 2 elements. Show that there is an element of G with no fixed points in S.

19 Question 19

Let $F \subset K \subset L$ be finite degree field extensions. For each of the following assertions, give a proof or a counterexample.

(a) If L/F is Galois, then so is K/F.

(b) If L/F is Galois, then so is L/K.

(c) If K/F and L/K are both Galois, then so is L/F.

20 Question 20

Let V be a finite dimensional vector space over a field (the field is not necessarily algebraically closed).

Let $\phi : V \longrightarrow V$ be a linear transformation. Prove that there exists a decomposition of V as $V = U \oplus W$, where U and W are ϕ-invariant subspaces of V , $\phi|_U$ is nilpotent, and $\phi|_W$ is nonsingular.

21 Question 21

Let A be an $n \times n$ matrix.

(a) Suppose that v is a column vector such that the set $\{v, Av, ..., A^{n-1}v\}$ is linearly independent. Show that any matrix B that commutes with A is a polynomial in A.

(b) Show that there exists a column vector v such that the set $\{v, Av, ..., A^{n-1}v\}$ is linearly independent $\iff$ the characteristic polynomial of A equals the minimal polynomial of A.

22 Question 22

Let R be a commutative ring, and let M be an R-module. An R-submodule N of M is maximal if there is no R-module P with $N \subsetneq P \subsetneq M$.

(a) Show that an R-submodule N of M is maximal $\iff$ M/N is a simple R-module: i.e., M/N is nonzero and has no proper, nonzero R-submodules.

(b) Let M be a $\mathbb{Z}$-module. Show that a $\mathbb{Z}$-submodule N of M is maximal $\iff$ $\#M/N$ is a prime number.

(c) Let M be the $\mathbb{Z}$-module of all roots of unity in $\mathbb{C}$ under multiplication. Show that there is no maximal $\mathbb{Z}$-submodule of M.

23 Question 23

Let R be a commutative ring.

(a) Let $r \in R$. Show that the map

$$\begin{aligned} r\bullet : R &\longrightarrow R \\ x &\mapsto rx. \end{aligned}$$

is an R-module endomorphism of R.

(b) We say that r is a **zero-divisor** if r$\bullet$ is not injective. Show that if r is a zero-divisor and $r \neq 0$, then the kernel and image of R each consist of zero-divisors.

(c) Let $n \geq 2$ be an integer. Show: if R has exactly n zero-divisors, then $\#R \leq n^2$.

(d) Show that up to isomorphism there are exactly two commutative rings R with precisely 2 zero-divisors.

You may use without proof the following fact: every ring of order 4 is isomorphic to exactly one of the following:

$$\frac{\mathbb{Z}}{4\mathbb{Z}}, \quad \frac{\frac{\mathbb{Z}}{2\mathbb{Z}}[t]}{(t^2+t+1)}, \quad \frac{\frac{\mathbb{Z}}{2\mathbb{Z}}[t]}{(t^2-t)}, \quad \frac{\frac{\mathbb{Z}}{2\mathbb{Z}}[t]}{(t^2)}.$$

24 Question 24

(a) Use the Class Equation (equivalently, the conjugation action of a group on itself) to prove that any p-group (a group whose order is a positive power of a prime integer p) has a nontrivial center.

(b) Prove that any group of order p^2 (where p is prime) is abelian.

(c) Prove that any group of order $5^2 \cdot 7^2$ is abelian.

(d) Write down exactly one representative in each isomorphism class of groups of order $5^2 \cdot 7^2$.

25 Question 25

Let $f(x) = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$.

(a) Find the splitting field K of f, and compute $[K : \mathbb{Q}]$.

(b) Find the Galois group G of f, both as an explicit group of automorphisms, and as a familiar abstract group to which it is isomorphic.

(c) Exhibit explicitly the correspondence between subgroups of G and intermediate fields between $\mathbb{Q}$ and k.

26 Question 26

Let K be a Galois extension of $\mathbb{Q}$ with Galois group G, and let E_1, E_2 be intermediate fields of K which are the splitting fields of irreducible $f_i(x) \in \mathbb{Q}[x]$.

Let $E = E_1E_2 \subset K$.

Let $H_i = \mathrm{Gal}(K/E_i)$ and $H = \mathrm{Gal}(K/E)$.

(a) Show that $H = H_1 \cap H_2$.

(b) Show that H_1H_2 is a subgroup of G.

(c) Show that

$$\mathrm{Gal}(K/(E_1 \cap E_2)) = H_1H_2.$$

27 Question 27

Let

$$A = \begin{bmatrix} 0 & 1 & -2 \\ 1 & 1 & -3 \\ 1 & 2 & -4 \end{bmatrix} \in M_3(\mathbb{C})$$

(a) Find the Jordan canonical form J of A.

(b) Find an invertible matrix P such that $P^{-1}AP = J$.

You should not need to compute P^{-1}.

28 Question 28

Let

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{and} \quad N = \begin{pmatrix} x & u \\ -y & -v \end{pmatrix}$$

over a commutative ring R, where b and x are units of R. Prove that

$$MN = \begin{pmatrix} 0 & 0 \\ 0 & * \end{pmatrix} \implies MN = 0.$$

29 Question 29

Let

$$M = \{(w, x, y, z) \in \mathbb{Z}^4 \mid w + x + y + z \in 2\mathbb{Z}\},$$

and

$$N = \{(w, x, y, z) \in \mathbb{Z}^4 \mid 4 \mid (w - x),\ 4 \mid (x - y),\ 4 \mid (y - z)\}.$$

(a) Show that N is a $\mathbb{Z}$-submodule of M .

(b) Find vectors $u_1, u_2, u_3, u_4 \in \mathbb{Z}^4$ and integers d_1, d_2, d_3, d_4 such that

$$\{u_1, u_2, u_3, u_4\}$$

is a free basis for M, and

$$\{d_1u_1,\ d_2u_2,\ d_3u_3,\ d_4u_4\}$$

is a free basis for N .

(c) Use the previous part to describe M/N as a direct sum of cyclic $\mathbb{Z}$-modules.

30 Question 30

Let R be a PID and M be an R-module. Let p be a prime element of R. The module M is called $\langle p \rangle$ *-primary* if for every $m \in M$ there exists $k > 0$ such that $p^k m = 0$.

(a) Suppose M is $\langle p \rangle$-primary. Show that if $m \in M$ and $t \in R$, $t \notin \langle p \rangle$, then there exists $a \in R$ such that $atm = m$.

(b) A submodule S of M is said to be *pure* if $S \cap rM = rS$ for all $r \in R$. Show that if M is $\langle p \rangle$-primary, then S is pure if and only if $S \cap p^k M = p^k S$ for all $k \geq 0$.

31 Question 31

Let $R = C[0, 1]$ be the ring of continuous real-valued functions on the interval $[0, 1]$. Let I be an ideal of R.

(a) Show that if $f \in I, a \in [0, 1]$ are such that $f(a) \neq 0$, then there exists $g \in I$ such that $g(x) \geq 0$ for all $x \in [0, 1]$, and $g(x) > 0$ for all x in some open neighborhood of a.

(b) If $I \neq R$, show that the set $Z(I) = \{x \in [0, 1] \mid f(x) = 0 \text{ for all } f \in I\}$ is nonempty.

(c) Show that if I is maximal, then there exists $x_0 \in [0, 1]$ such that $I = \{f \in R \mid f(x_0) = 0\}$.

32 Question 32

Suppose the group G acts on the set A. Assume this action is faithful (recall that this means that the kernel of the homomorphism from G to $\mathrm{Sym}(A)$ which gives the action is trivial) and transitive (for all a, b in A, there exists g in G such that $g \cdot a = b$.)

(a) For $a \in A$, let G_a denote the stabilizer of a in G. Prove that for any $a \in A$,

$$\bigcap_{\sigma \in G} \sigma G_a \sigma^{-1} = \{1\}.$$

(b) Suppose that G is abelian. Prove that $|G| = |A|$. Deduce that every abelian transitive subgroup of S_n has order n.

33 Question 33

(a) Classify the abelian groups of order 36.

For the rest of the problem, assume that G is a non-abelian group of order 36.

> You may assume that the only subgroup of order 12 in S_4 is A_4 and that A_4 has no subgroup of order 6.

(b) Prove that if the 2-Sylow subgroup of G is normal, G has a normal subgroup N such that G/N is isomorphic to A_4.

(c) Show that if G has a normal subgroup N such that G/N is isomorphic to A_4 and a subgroup \$H isomorphic to A_4 it must be the direct product of N and H.

(d) Show that the dihedral group of order 36 is a non-abelian group of order 36 whose Sylow-2 subgroup is not normal.

34 Question 34

Let F be a field. Let $f(x)$ be an irreducible polynomial in $F[x]$ of degree n and let $g(x)$ be any polynomial in $F[x]$. Let $p(x)$ be an irreducible factor (of degree m) of the polynomial $f(g(x))$.

Prove that n divides m. Use this to prove that if r is an integer which is not a perfect square, and n is a positive integer then every irreducible factor of $x^{2n} - r$ over $\mathbb{Q}[x]$ has even degree.

35 Question 35

(a) Let $f(x)$ be an irreducible polynomial of degree 4 in $\mathbb{Q}[x]$ whose splitting field K over $\mathbb{Q}$ has Galois group $G = S_4$.

Let θ be a root of $f(x)$. Prove that $\mathbb{Q}[\theta]$ is an extension of $\mathbb{Q}$ of degree 4 and that there are no intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}[\theta]$.

(b) Prove that if K is a Galois extension of $\mathbb{Q}$ of degree 4, then there is an intermediate subfield between K and $\mathbb{Q}$.

36 Question 36

A ring R is called *simple* if its only two-sided ideals are 0 and R.

(a) Suppose R is a commutative ring with 1. Prove R is simple if and only if R is a field.

(b) Let k be a field. Show the ring $M_n(k)$, $n \times n$ matrices with entries in k, is a simple ring.

37 Question 37

For a ring R, let $U(R)$ denote the multiplicative group of units in R. Recall that in an integral domain R, $r \in R$ is called *irreducible* if r is not a unit in R, and the only divisors of r have the form ru with u a unit in R.

We call a non-zero, non-unit $r \in R$ *prime* in R if $r \,\Big|\, ab \implies r \,\Big|\, a$ or $r \,\Big|\, b$. Consider the ring $R = \{a + b\sqrt{-5} \,\Big|\, a, b \in Z\}$.

(a) Prove R is an integral domain.

(b) Show $U(R) = \{\pm 1\}$.

(c) Show $3, 2 + \sqrt{-5}$, and $2 - \sqrt{-5}$ are irreducible in R.

(d) Show 3 is not prime in R.

(e) Conclude R is not a PID.

38 Question 38

Let F be a field and let V and W be vector spaces over F .

Make V and W into $F[x]$-modules via linear operators T on V and S on W by defining $X \cdot v = T(v)$ for all $v \in V$ and $X \cdot w = S(w)$ for all w ∈ W .

Denote the resulting $F[x]$-modules by V_T and W_S respectively.

(a) Show that an $F[x]$-module homomorphism from V_T to W_S consists of an F-linear transformation $R : V \longrightarrow W$ such that $RT = SR$.

(b) Show that $VT \cong WS$ as $F[x]$-modules $\iff$ there is an F-linear isomorphism $P : V \longrightarrow W$ such that $T = P^{-1}SP$.

(c) Recall that a module M is *simple* if $M \neq 0$ and any proper submodule of M must be zero. Suppose that V has dimension 2. Give an example of F, T with V_T simple.

(d) Assume F is algebraically closed. Prove that if V has dimension 2, then any V_T is not simple.

39 Question 39

40 Question 40

41 Question 41

42 Question 42

Show that no finite group is the union of conjugates of a proper subgroup.

43 Question 43

Classify all groups of order 18 up to isomorphism.

44 Question 44

Let α, β denote the unique positive real 5^{th} root of 7 and 4^{th} root of 5, respectively. Determine the degree of $\mathbb{Q}(\alpha, \beta)$ over $\mathbb{Q}$.

45 Question 45

Show that the field extension $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$ is Galois and determine its Galois group.

46 Question 46

Let M be a square matrix over a field K. Use a suitable canonical form to show that M is similar to its transpose M^T.

47 Question 47

Let G be a finite group and π_0, π_1 be two irreducible representations of G. Prove or disprove the following assertion: π_0 and π_1 are equivalent if and only if $\det \pi_0(g) = \det \pi_1(g)$ for all $g \in G$.

48 Question 48

Let R be a Noetherian ring. Prove that $R[x]$ and $R[[x]]$ are both Noetherian. (The first part of the question is asking you to prove the Hilbert Basis Theorem, not to use it!)

49 Question 49

Classify (with proof) all fields with finitely many elements.

50 Question 50

Suppose A is a commutative ring and M is a finitely presented module. Given any surjection $\phi : A^n \to M$ from a finite free A-module, show that $\ker \phi$ is finitely generated.

51 Question 51

Classify all groups of order 57.

52 Question 52

Show that a finite simple group cannot have a 2-dimensional irreducible representation over $\mathbb{C}$. (Hint: the determinant might prove useful.)

53 Question 53

Let G be a finite simple group. Assume that every proper subgroup of G is abelian. Prove that then G is cyclic of prime order.

54 Question 54

Let $a \in \mathbb{N}$, $a > 0$. Compute the Galois group of the splitting field of the polynomial $x^5 - 5a^4x + a$ over $\mathbb{Q}$.

55 Question 55

Recall that an inner automorphism of a group is an automorphism given by conjugation by an element of the group. An outer automorphism is an automorphism that is not inner.

- Prove that S_5 has a subgroup of order 20.
- Use the subgroup from (a) to construct a degree 6 permutation representation of S_5 (i.e., an embedding $S_5 \hookrightarrow S_6$ as a transitive permutation group on 6 letters).
- Conclude that S_6 has an outer automorphism.

56 Question 56

Let A be a commutative ring and M a finitely generated A-module. Define

$$\mathrm{Ann}(M) = \{a \in A : am = 0 \text{ for all } m \in M\}.$$

Show that for a prime ideal $\mathfrak{p} \subset A$, the following are equivalent:

- $\mathrm{Ann}(M) \not\subset \mathfrak{p}$
- The localization of M at the prime ideal $\mathfrak{p}$ is 0.
- $M \otimes_A k(\mathfrak{p}) = 0$, where $k(\mathfrak{p}) = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ is the residue field of A at $\mathfrak{p}$.

57 Question 57

Let $A = \mathbb{C}[x, y]/(y^2 - (x - 1)^3 - (x - 1)^2)$.

- Show that A is an integral domain and sketch the $\mathbb{R}$-points of $\mathrm{Spec}A$.
- Find the integral closure of A. Recall that for an integral domain A with fraction field K, the integral closure of A in K is the set of all elements of K integral over A.

58 Question 58

Let $R = k[x, y]$ where k is a field, and let $I = (x, y)R$.

- Show that

  $$0 \longrightarrow R \xrightarrow{\phi} R \oplus R \xrightarrow{\psi} R \longrightarrow k \longrightarrow 0$$

  where $\phi(a) = (-ya, xa)$, $\psi((a, b)) = xa + yb$ for $a, b \in R$, is a projective resolution of the R-module $k \simeq R/I$.
- Show that I is not a flat R-module by computing $\mathrm{Tor}_i^R(I, k)$

59 Question 59

- Find an irreducible polynomial of degree 5 over the field $\mathbb{Z}/2$ of two elements and use it to construct a field of order 32 as a quotient of the polynomial ring $\mathbb{Z}/2[x]$.
- Using the polynomial found in part (a), find a 5×5 matrix M over $\mathbb{Z}/2$ of order 31, so that $M^{31} = I$ but $M \neq I$.

60 Question 60

Find the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$. Justify your answer.

61 Question 61

- Let R be a commutative ring with no nonzero nilpotent elements. Show that the only units in the polynomial ring $R[x]$ are the units of R, regarded as constant polynomials.
- Find all units in the polynomial ring $\mathbb{Z}_4[x]$.

62 Question 62

Let p, q be two distinct primes. Prove that there is at most one non-abelian group of order pq and describe the pairs (p, q) such that there is no non-abelian group of order pq.

63 Question 63

- Let L be a Galois extension of a field K of degree 4. What is the minimum number of subfields there could be strictly between K and L? What is the maximum number of such subfields? Give examples where these bounds are attained.
- How do these numbers change if we assume only that L is separable (but not necessarily Galois) over K?

64 Question 64

Let R be a commutative algebra over $\mathbb{C}$. A derivation of R is a $\mathbb{C}$-linear map $D : R \to R$ such that (i) $D(1) = 0$ and (ii) $D(ab) = D(a)b + aD(b)$ for all $a, b \in R$.

- Describe all derivations of the polynomial ring $\mathbb{C}[x]$.
- Let A be the subring (or $\mathbb{C}$-subalgebra) of $\mathrm{End}_{\mathbb{C}}(\mathbb{C}[x])$ generated by all derivations of $\mathbb{C}[x]$ and the left multiplications by x. Prove that $\mathbb{C}[x]$ is a simple left A-module. > Note that the inclusion $A \to \mathrm{End}_{\mathbb{C}}(\mathbb{C}[x])$ defines a natural left A-module structure on $\mathbb{C}[x]$.

65 Question 65

Let G be a non-abelian group of order p^3 with p a prime.

- Determine the order of the center Z of G.
- Determine the number of inequivalent complex 1-dimensional representations of G.
- Compute the dimensions of all the inequivalent irreducible representations of G and verify that the number of such representations equals the number of conjugacy classes of G.

66 Question 66

- Let G be a group (not necessarily finite) that contains a subgroup of index n. Show that G contains a *normal* subgroup N such that $n \leq [G : N] \leq n!$
- Use part (a) to show that there is no simple group of order 36.

67 Question 67

Let p be a prime, let $\mathbb{F}_p$ be the p-element field, and let $K = \mathbb{F}_p(t)$ be the field of rational functions in t with coefficients in $\mathbb{F}_p$. Consider the polynomial $f(x) = x^p - t \in K[x]$.

- Show that f does not have a root in K.
- Let E be the splitting field of f over K. Find the factorization of f over E.
- Conclude that f is irreducible over K.

68 Question 68

Recall that a ring A is called *graded* if it admits a direct sum decomposition $A = \oplus_{n=0}^{\infty} A_n$ as abelian groups, with the property that $A_i A_j \subseteq A_{i+j}$ for all $i, j \geq 0$. Prove that a graded commutative ring $A = \oplus_{n=0}^{\infty} A_n$ is Noetherian if and only if A_0 is Noetherian and A is finitely generated as an algebra over A_0.

69 Question 69

Let R be a ring with the property that $a^2 = a$ for all $a \in R$.

- Compute the Jacobson radical of R.
- What is the characteristic of R?
- Prove that R is commutative.
- Prove that if R is finite, then R is isomorphic (as a ring) to $(\mathbb{Z}/2\mathbb{Z})^d$ for some d.

70 Question 70

Let $\overline{\mathbb{F}_p}$ denote the algebraic closure of $\mathbb{F}_p$. Show that the Galois group $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ has no non-trivial finite subgroups.

71 Question 71

Let C_p denote the cyclic group of order p.

- Show that C_p has two irreducible representations over $\mathbb{Q}$ (up to isomorphism), one of dimension 1 and one of dimension $p - 1$.

- Let G be a finite group, and let $\rho : G \to \mathrm{GL}_n(\mathbb{Q})$ be a representation of G over $\mathbb{Q}$. Let $\rho_{\mathbb{C}} : G \to \mathrm{GL}_n(\mathbb{C})$ denote ρ followed by the inclusion $\mathrm{GL}_n(\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$. Thus $\rho_{\mathbb{C}}$ is a representation of G over $\mathbb{C}$, called the *complexification* of ρ. We say that an irreducible representation ρ of G is *absolutely irreducible* if its complexification remains irreducible over $\mathbb{C}$.\ Now suppose G is abelian and that every representation of G over $\mathbb{Q}$ is absolutely irreducible. Show that $G \cong (C_2)^k$ for some k (i.e., is a product of cyclic groups of order 2).

72 Question 72

Let G be a finite group and $\mathbb{Z}[G]$ the internal group algebra. Let $\mathcal{Z}$ be the center of $\mathbb{Z}[G]$. For each conjugacy class $C \subseteq G$, let $P_C = \sum_{g \in C} g$.

- Show that the elements P_C form a $\mathbb{Z}$-basis for $\mathcal{Z}$. Hence $\mathcal{Z} \cong \mathbb{Z}^d$ as an abelian group, where d is the number of conjugacy classes in G.
- Show that if a ring R is isomorphic to $\mathbb{Z}^d$ as an abelian group, then every element in R satisfies a monic integral polynomial. (**Hint:** Let $\{v_1, \ldots, v_d\}$ be a basis of R and for a fixed non-zero $r \in R$, write $rv_i = \sum_j a_{ij} v_j$. Use the Hamilton-Cayley theorem.)
- Let $\pi : G \to \mathrm{GL}(V)$ be an irreducible representation of G (over $\mathbb{C}$). Show that $\pi(P_C)$ acts on V as multiplication by the scalar

$$\frac{|C|\chi_\pi(C)}{\dim V},$$

  where $\chi_\pi(C)$ is the value of the character χ_π on any element of C.
- Conclude that $|C|\chi_\pi(C)/\dim V$ is an algebraic integer.

73 Question 73

- Suppose that G is a finitely generated group. Let n be a positive integer. Prove that G has only finitely many subgroups of index n
- Let p be a prime number. If G is any finitely-generated abelian group, let $t_p(G)$ denote the number of subgroups of G of index p. Determine the possible values of $t_p(G)$ as G varies over all finitely-generated abelian groups.

74 Question 74

- Suppose that G is a finitely generated group. Let n be a positive integer. Prove that G has only finitely many subgroups of index n
- Let p be a prime number. If G is any finitely-generated abelian group, let $t_p(G)$ denote the number of subgroups of G of index p. Determine the possible values of $t_p(G)$ as G varies over all finitely-generated abelian groups.

75 Question 75

Suppose that G is a finite group of order 2013. Prove that G has a normal subgroup N of index 3 and that N is a cyclic group. Furthermore, prove that the center of G has order divisible by 11. (You will need the factorization $2013 = 3 \cdot 11 \cdot 61$.)

76 Question 76

This question concerns an extension K of $\mathbb{Q}$ such that $[K : \mathbb{Q}] = 8$. Assume that $K/\mathbb{Q}$ is Galois and let $G = \mathrm{Gal}(K/\mathbb{Q})$. Furthermore, assume that G is non-abelian.

- Prove that K has a unique subfield F such that $F/\mathbb{Q}$ is Galois and $[F : \mathbb{Q}] = 4$.
- Prove that F has the form $F = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ where d_1, d_2 are non-zero integers.
- Suppose that G is the quaternionic group. Prove that d_1 and d_2 are positive integers.

77 Question 77

This question concerns the polynomial ring $R = \mathbb{Z}[x, y]$ and the ideal $I = (5, x^2 + 2)$ in R.

- Prove that I is a prime ideal of R and that R/I is a PID.
- Give an explicit example of a maximal ideal of R which contains I. (Give a set of generators for such an ideal.)
- Show that there are infinitely many distinct maximal ideals in R which contain I.

78 Question 78

Classify all groups of order 2012 up to isomorphism. (Hint: 503 is prime).

79 Question 79

For any positive integer n, let G_n be the group generated by a and b subject to the following three relations:

$$a^2 = 1, \quad b^2 = 1, \quad \text{and} \quad (ab)^n = 1.$$

- Find the order of the group G_n

80 Question 80

Determine the Galois groups of the following polynomials over $\mathbb{Q}$.

- $f(x) = x^4 + 4x^2 + 1$
- $f(x) = x^4 + 4x^2 - 5$.

81 Question 81

Let R be a (commutative) principal ideal domain, let M and N be finitely generated free R-modules, and let $\varphi : M \to N$ be an R-module homomorphism.

- Let K be the kernel of φ. Prove that K is a direct summand of M.
- Let C be the image of φ. Show by example (specifying R, M, N, and φ) that C need not be a direct summand of N.

82 Question 82

In this problem, as you apply Sylow's Theorem, state precisely which portions you are using.

- Prove that there is no simple group of order 30.
- Suppose that G is a simple group of order 60. Determine the number of p-Sylow subgroups of G for each prime p dividing 60, then prove that G is isomorphic to the alternating group A_5.

> Note: in the second part, you needn't show that A_5 is simple. You need only show that if there is a simple group of order 60, then it must be isomorphic to A_5.

83 Question 83

Describe the Galois group and the intermediate fields of the cyclotomic extension $\mathbb{Q}(\zeta_{12})/\mathbb{Q}$.

84 Question 84

Let

$$R = \mathbb{Z}[x]/(x^2 + x + 1).$$

- Answer the following questions with suitable justification.
  - Is R a Noetherian ring?
  - Is R an Artinian ring?
- Prove that R is an integrally closed domain.

85 Question 85

Let R be a commutative ring. Recall that an element r of R is *nilpotent* if $r^n = 0$ for some positive integer n and that the *nilradical* of R is the set $N(R)$ of nilpotent elements.

- Prove that

$$N(R) = \cap_{P \text{ prime}} P.$$

  (Hint: given a non-nilpotent element r of R, you may wish to construct a prime ideal that does not contain r or its powers.)

- Given a positive integer m, determine the nilradical of $\mathbb{Z}/(m)$.
- Determine the nilradical of $\mathbb{C}[x,y]/(y^2-x^3)$.
- Let $p(x,y)$ be a polynomial in $\mathbb{C}[x,y]$ such that for any complex number a, $p(a,a^{3/2})=0$. Prove that $p(x,y)$ is divisible by y^2-x^3.

86 Question 86

Given a finite group G, recall that its *regular representation* is the representation on the complex group algebra $\mathbb{C}[G]$ induced by left multiplication of G on itself and its *adjoint representation* is the representation on the complex group algebra $\mathbb{C}[G]$ induced by conjugation of G on itself.

- Let $G=\mathrm{GL}_2(\mathbb{F}_2)$. Describe the number and dimensions of the irreducible representations of G. Then describe the decomposition of its regular representation as a direct sum of irreducible representations.
- Let G be a group of order 12. Show that its adjoint representation is reducible; that is, there is an H-invariant subspace of $\mathbb{C}[H]$ besides 0 and $\mathbb{C}[H]$.

87 Question 87

Let R be a commutative integral domain. Show that the following are equivalent:

- R is a field;
- R is a semi-simple ring;
- Any R-module is projective.

88 Question 88

Let p be a positive prime number, $\mathbb{F}_p$ the field with p elements, and let $G=\mathrm{GL}_2(\mathbb{F}_p)$.

- Compute the order of G, $|G|$.
- Write down an explicit isomorphism from $\mathbb{Z}/p\mathbb{Z}$ to
$$U=\left\{\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}\,\middle|\, a\in\mathbb{F}_p\right\}.$$
- How many subgroups of order p does G have? Hint: compute gug^{-1} for $g\in G$ and $u\in U$; use this to find the size of the normalizer of U in G.

89 Question 89

- Give definitions of the following terms:
  (i) a finite length (left) module, (ii) a composition series for a module, and (iii) the length of a module,

- Let $l(M)$ denote the length of a module M. Prove that if

$$0 \to M_1 \to M_2 \to \cdots \to M_n \to 0$$

is an exact sequence of modules of finite length, then

$$\sum_{i=1}^{n}(-1)^k l(M_i) = 0.$$

90 Question 90

Let $\mathbb{F}$ be a field of characteristic p, and G a group of order p^n. Let $R = \mathbb{F}[G]$ be the group ring (group algebra) of G over $\mathbb{F}$, and let $u := \sum_{x \in G} x$ (so u is an element of R).

- Prove that u lies in the center of R.
- Verify that Ru is a 2-sided ideal of R.
- Show there exists a positive integer k such that $u^k = 0$. Conclude that for such a k, $(Ru)^k = 0$.
- Show that R is **not** a semi-simple ring. (**Warning:** Please use the definition of a semi-simple ring: do **not** use the result that a finite length ring fails to be semisimple if and only if it has a non-zero nilpotent ideal.)

91 Question 91

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ (where $a_n \neq 0$) and let $R = \mathbb{Z}[x]/(f)$. Prove that R is a finitely generated module over $\mathbb{Z}$ if and only if $a_n = \pm 1$.

92 Question 92

Consider the ring

$$S = C[0,1] = \{f : [0,1] \to \mathbb{R} : f \text{ is continuous}\}$$

with the usual operations of addition and multiplication of functions.

- What are the invertible elements of S?
- For $a \in [0,1]$, define $I_a = \{f \in S : f(a) = 0\}$. Show that I_a is a maximal ideal of S.
- Show that the elements of any proper ideal of S have a common zero, i.e., if I is a proper ideal of S, then there exists $a \in [0,1]$ such that $f(a) = 0$ for all $f \in I$. Conclude that every maximal ideal of S is of the form I_a for some $a \in [0,1]$. **Hint:** as $[0,1]$ is compact, every open cover of $[0,1]$ contains a finite subcover.

93 Question 93

Let F be a field of characteristic zero, and let K be an *algebraic* extension of F that possesses the following property: every polynomial $f \in F[x]$ has a root in K. Show that K is algebraically closed.\ **Hint:** if $K(\theta)/K$ is algebraic, consider $F(\theta)/F$ and its normal closure; primitive elements might be of help.

94 Question 94

Let G be the unique non-abelian group of order 21.

- Describe all 1-dimensional complex representations of G.
- How many (non-isomorphic) irreducible complex representations does G have and what are their dimensions?
- Determine the character table of G.

95 Question 95

- Classify all groups of order $2009 = 7^2 \times 41$.
- Suppose that G is a group of order 2009. How many intermediate groups are there—that is, how many groups H are there with $1 \subsetneq H \subsetneq G$, where both inclusions are proper? (There may be several cases to consider.)

96 Question 96

Let K be a field. A discrete valuation on K is a function $\nu : K \setminus \{0\} \to \mathbb{Z}$ such that

- $\nu(ab) = \nu(a) + \nu(b)$
- ν is surjective
- $\nu(a+b) \geq \min\{(\nu(a), \nu(b)\}$ for $a, b \in K \setminus \{0\}$ with $a + b \neq 0$.

Let $R := \{x \in K \setminus \{0\} : \nu(x) \geq 0\} \cup \{0\}$. Then R is called the valuation ring of ν.

Prove the following:

- R is a subring of K containing the 1 in K.
- for all $x \in K \setminus \{0\}$, either x or x^{-1} is in R.
- x is a unit of R if and only if $\nu(x) = 0$.
- Let p be a prime number, $K = \mathbb{Q}$, and $\nu_p : \mathbb{Q} \setminus \{0\} \to \mathbb{Z}$ be the function defined by $\nu_p(\frac{a}{b}) = n$ where $\frac{a}{b} = p^n \frac{c}{d}$ and p does not divide c and d. Prove that the corresponding valuation ring R is the ring of all rational numbers whose denominators are relatively prime to p.

97 Question 97

Let F be a field of characteristic not equal to 2.

- Prove that any extension K of F of degree 2 is of the form $F(\sqrt{D})$ where $D \in F$ is not a square in F and, conversely, that each such extension has degree 2 over F.
- Let $D_1, D_2 \in F$ neither of which is a square in F. Prove that $[F(\sqrt{D_1}, \sqrt{D_2}) : F] = 4$ if $D_1 D_2$ is not a square in F and is of degree 2 otherwise.

98 Question 98

Let F be a field and $p(x) \in F[x]$ an irreducible polynomial.

- Prove that there exists a field extension K of F in which $p(x)$ has a root.
- Determine the dimension of K as a vector space over F and exhibit a vector space basis for K.
- If $\theta \in K$ denotes a root of $p(x)$, express θ^{-1} in terms of the basis found in part (b).
- Suppose $p(x) = x^3 + 9x + 6$. Show $p(x)$ is irreducible over $\mathbb{Q}$. If θ is a root of $p(x)$, compute the inverse of $(1 + \theta)$ in $\mathbb{Q}(\theta)$.

99 Question 99

Fix a ring R, an R-module M, and an R-module homomorphism $f : M \to M$.

- If M satisfies the descending chain condition on submodules, show that if f is injective, then f is surjective. (Hint: note that if f is injective, so are $f \circ f$, $f \circ f \circ f$, etc.)
- Give an example of a ring R, an R-module M, and an injective R-module homomorphism $f : M \to M$ which is not surjective.
- If M satisfies the ascending chain condition on submodules, show that if f is surjective, then f is injective.
- Give an exampe of a ring R, and R-module M, and a surjective R-module homomorphism $f : M \to M$ which is not injective.

100 Question 100

Let G be a finite group, k an algebraically closed field, and V an irreducible k-linear representation of G.

- Show that $\hom_{kG}(V, V)$ is a division algebra with k in its center.
- Show that V is finite-dimensional over k, and conclude that $\hom_{kG}(V, V)$ is also finite dimensional.
- Show the inclusion $k \hookrightarrow \hom_{kG}(V, V)$ found in (a) is an isomorphism. (For $f \in \hom_{kG}(V, V)$, view f as a linear transformation and consider $f - \alpha I$, where α is an eigenvalue of f).

101 Question 101

Let $f(x)$ be an irreducible polynomial of degree 5 over the field $\mathbb{Q}$ of rational numbers with exactly 3 real roots.

- Show that $f(x)$ is not solvable by radicals.
- Let E be the splitting field of f over $\mathbb{Q}$. Construct a Galois extension K of degree 2 over $\mathbb{Q}$ lying in E such that *no* field F strictly between K and E is Galois over $\mathbb{Q}$.

102 Question 102

Let F be a finite field. Show for any positive integer n that there are irreducible polynomials of degree n in $F[x]$.

103 Question 103

Show that the order of the group $\mathrm{GL}_n(\mathbb{F}_q)$ of invertible $n \times n$ matrices over the field $\mathbb{F}_q$ of q elements is given by $(q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$.

104 Question 104

- Let R be a commutative principal ideal domain. Show that any R-module M generated by two elements takes the form $R/(a) \oplus R/(b)$ for some $a, b \in R$. What more can you say about a and b?
- Give a necessary and sufficient condition for two direct sums as in part (a) to be isomorphic as R-modules.

105 Question 105

Let G be the subgroup of $\mathrm{GL}_3(\mathbb{C})$ generated by the three matrices

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} i & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

where $i^2 = -1$. Here $\mathbb{C}$ denotes the complex field.

- Compute the order of G.
- Find a matrix in G of largest possible order (as an element of G) and compute this order.
- Compute the number of elements in G with this largest order.

106 Question 106

- Let G be a group of (finite) order n. Show that any irreducible left module over the group algebra $\mathbb{C}G$ has complex dimension at least $\sqrt{n}$.
- Give an example of a group G of order $n \geq 5$ and an irreducible left module over $\mathbb{C}G$ of complex dimension $\lfloor \sqrt{n} \rfloor$, the greatest integer to $\sqrt{n}$.

107 Question 107

Use the rational canonical form to show that any square matrix M over a field k is similar to its transpose M^t, recalling that $p(M) = 0$ for some $p \in k[t]$ if and only if $p(M^t) = 0$.

108 Question 108

Let K be a field of characteristic zero and L a Galois extension of K. Let f be an irreducible polynomial in $K[x]$ of degree 7 and suppose f has no zeroes in L. Show that f is irreducible in $L[x]$.

109 Question 109

Let K be a field of characteristic zero and $f \in K[x]$ an irreducible polynomial of degree n. Let L be a splitting field for f. Let G be the group of automorphisms of L which act trivially on K.

- Show that G embeds in the symmetric group S_n.
- For each n, give an example of a field K and polynomial f such that $G = S_n$.
- What are the possible groups G when $n = 3$. Justify your answer.

110 Question 110

Show there are exactly two groups of order 21 up to isomorphism.

111 Question 111

Let K be the field $\mathbb{Q}(z)$ of rational functions in a variable z with coeffiecients in the rational field $\mathbb{Q}$. Let n be a positive integer. Consider the polynomial $x^n - z \in K[x]$.

- Show that the polynomial $x^n - z$ is irreducible over K.
- Describe the splitting field of $x^n - z$ over K.
- Determine the Galois group of the splitting field of $x^5 - z$ over the field K.

112 Question 112

- Let $p < q < r$ be prime integers. Show that a group of order pqr cannot be simple.
- Consider groups of orders $2^2 \cdot 3 \cdot p$ where p has the values 5, 7, and 11. For each of those values of p, either display a simple group of order $2^2 \cdot 3 \cdot p$, or show that there cannot be a simple group of that order.

113 Question 113

Let K/F be a finite Galois extension and let $n = [K : F]$. There is a theorem (often referred to as the "normal basis theorem") which states that there exists an irreducible polynomial $f(x) \in F[x]$ whose roots form a basis for K as a vector space over F. You may assume that theorem in this problem.

- Let $G = \mathrm{Gal}(K/F)$. The action of G on K makes K into a finite-dimensional representation space for G over F. Prove that K is isomorphic to the regular representation for G over F.

  > The regular representation is defined by letting G act on the group algebra $F[G]$ by multiplication on the left.

- Suppose that the Galois group G is cyclic and that F contains a primitive n^{th} root of unity. Show that there exists an injective homomorphism $\chi : G \to F^\times$.
- Show that K contains a non-zero element a with the following property:

  $$g(a) = \chi(g) \cdot a$$

  for all $g \in G$.
- If a has the property stated in (c), show that $K = F(a)$ and that $a^n \in F^\times$.

114 Question 114

Let G be the group of matrices of the form

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

with entries in the finite field $\mathbb{F}_p$ of p element, where p is a prime.

- Prove that G is non-abelian.
- Suppose p is odd. Prove that $g^p = I_3$ for all $g \in G$.
- Suppose that $p = 2$. It is known that there are exactly two non-abelian groups of order 8, up to isomorphism: the dihedral group D_8 and the quaternionic group. Assuming this fact without proof, determine which of these groups G is isomorphic to.

115 Question 115

There are five nonisomorphic groups of order 8. For each of those groups G, find the smallest positive integer n such that there is an injective homomorphism $\varphi : G \to S_n$.

116 Question 116

For any group G we define $\Omega(G)$ to be the image of the group homomorphism $\rho : G \to \mathrm{Aut}(G)$ where ρ maps $g \in G$ to the conjugation automorphism $x \mapsto gxg^{-1}$. Starting with a group G_0, we define $G_1 = \Omega(G_0)$ and $G_{i+1} = \Omega(G_i)$ for all $i \geq 0$. If G_0 is of order p^e for a prime p and integer $e \geq 2$, prove that G_{e-1} is the trivial group.

117 Question 117

Let $\mathbb{F}_2$ be the field with two elements.

- What is the order of $\mathrm{GL}_3(\mathbb{F}_2)$?
- Use the fact that $\mathrm{GL}_3(\mathbb{F}_2)$ is a simple group (which you should not prove) to find the number of elements of order 7 in $\mathrm{GL}_3(\mathbb{F}_2)$.

118 Question 118

Let G be a finite abelian group. Let $f : \mathbb{Z}^m \to G$ be a surjection of abelian groups. We may think of f as a homomorphism of $\mathbb{Z}$-modules. Let K be the kernel of f.

- Prove that K is isomorphic to $\mathbb{Z}^m$.
- We can therefore write the inclusion map $K \to \mathbb{Z}^m$ as $\mathbb{Z}^m \to \mathbb{Z}^m$ and represent it by an $m \times m$ integer matrix A. Prove that $|\det A| = |G|$.

119 Question 119

Let $R = C([0, 1])$ be the ring of all continuous real-valued functions on the closed interval $[0, 1]$, and for each $c \in [0, 1]$, denote by M_c the set of all functions $f \in R$ such that $f(c) = 0$.

- Prove that $g \in R$ is a unit if and only if $g(c) \neq 0$ for all $c \in [0, 1]$.
- Prove that for each $c \in [0, 1]$, M_c is a maximal ideal of R.
- Prove that if M is a maximal ideal of T, then $M = M_c$ for some $c \in [0, 1]$. (Hint: compactness of $[0, 1]$ may be relevant.)

120 Question 120

Let R and S be commutative rings, and $f : R \to S$ a ring homomorphism.

- Show that if I is a prime ideal of S, then

$$f^{-1}(I) = \{r \in R : f(r) \in I\}$$

is a prime ideal of R.

- Let N be the set of nilpotent elements of R:

$$N = \{r \in R : r^m = 0 \text{ for some } m \geq 1\}.$$

N is called the *nilradical* of R. Prove that it is an ideal which is contained in every prime ideal.

- Part (a) lets us define a function

$$f^* : \{\text{prime ideals of } S\} \to \{\text{prime ideals of } R\}.$$

$$I \mapsto f^{-1}(I).$$

Let N be the nilradical of R. Show that if $S = R/N$ and $f : R \to R/N$ is the quotient map, then f^* is a bijection

121 Question 121

Consider the polynomial $f(x) = x^{10} + x^5 + 1 \in \mathbb{Q}[x]$ with splitting field K over $\mathbb{Q}$.

- Determine whether $f(x)$ is irreducible over $\mathbb{Q}$ and find $[K : \mathbb{Q}]$.
- Determine the structure of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$.

122 Question 122

For each prime number p and each positive integer n, how many elements α are there in $\mathbb{F}_{p^n}$ such that $F_p(\alpha) = F_{p^6}$?

123 Question 123

Assume that K is a cyclic group, H is an arbitrary group, and φ_1 and φ_2 are homomorphisms from K into $\mathrm{Aut}(H)$ such that $\varphi_1(K)$ and $\varphi_2(K)$ are conjugate subgroups of $\mathrm{Aut}(H)$.

Prove by constructing an explicit isomorphism that $H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_2} K$.

> Suppose $\sigma_{\varphi_1}(K)\sigma^{-1} = \varphi_2(K)$ so that for some $a \in \mathbb{Z}$ we have $\sigma\varphi_1(k)\sigma^{-1} = \varphi_2(k)^a$ for all $k \in K$. Show that the map $\psi : H \rtimes_{\varphi_1} K \to H \rtimes_{\varphi_2} K$ defined by $\psi((h,k)) = (\sigma(h), k^a)$ is a homomorphism. Show ψ is bijective by construcing a 2-sided inverse.

124 Question 124

Something something G.

125 Question 125

Classify the groups of order $182 = 2 \cdot 7 \cdot 13$.

126 Question 126

Let G be a finite group of order $p^n m$ where p is a prime and m is not divisible by p. Prove that if H is a subgroup of G of order p^k for some $k < n$, then the normalizer of H in G properly contains H.

127 Question 127

Let H be a subgroup of S_n of index n. Prove:

1. There is an isomorphism $f : S_n \longrightarrow S_n$ such that $f(H)$ is the subgroup of S_n stabilizing n. In particular, H is isomorphic to S_{n-1}.
2. The only subgroups of S_n containing H are S_n and H.

128 Question 128

- Prove that a group of order $351 = 3^3 \cdot 13$ cannot be simple.
- Prove that a group of order 33 must be cyclic.

129 Question 129

1. Let G be a group, and $Z(G)$ the center of G. Prove that if $G/Z(G)$ is cyclic, then G is abelian.
2. Prove that a group of order p^n, where p is a prime and $n \geq 1$, has non-trivial center.
3. Prove that a group of order p^2 must be abelian.

130 Question 130

Let G be a finite group.

1. Prove that if $H < G$ is a proper subgroup, then G is not the union of conjugates of H.
2. Suppose that G acts transitively on a set X with $|X| > 1$. Prove that there exists an element of G with no fixed points in X.

131 Question 131

Classify all groups of order 15 and of order 30.

132 Question 132

Count the number of p-Sylow subgroups of S_p.

133 Question 133

1. Let G be a group of order n. Suppose that for every divisor d of n, G contains at most one subgroup of order d. Show that G is clyclic.
2. Let F be a field. Show that every finite subgroup of the group of units $F^\times$ is cyclic.

134 Question 134

Classify the groups of order $182 = 2 \cdot 7 \cdot 13$.