
Directions: Read ALL of the following directions.

This is an open-notes, open-homework, open-textbook exam. There is no official time limit, but it is suggested that you should be able to solve most of the problems within approximately 5 hours.

There are 7 problems totaling 100 points on this exam.

Justify any answers you give, including computations. You may freely refer to results from in class, from the course notes, course assignments and solutions, and the course textbook, but please make it clear what results you are using.

Proofs and explanations are expected to be clear, concise, and correct.

In problems with multiple parts, you MAY use the results of previous parts in later parts, even if you were unable to solve the earlier parts correctly.

You MAY use a computer for typesetting and to access any material on the course webpage (e.g., the course notes and homework solutions), and to perform computations. Any such computations must be clearly identified and justified as correct.

You MAY NOT use a computer to access any other information.

You MAY ask the instructor for help on any part of the exam, during office hours or via email. (The instructor may or may not decide to grant help, but you are encouraged to ask regardless.)

You MAY NOT discuss the material on this exam with anyone except for the instructor (until after the due date). This includes asking others for hints or solutions, searching for information about the problems online, or posting about the problems on discussion forums.

Please include AND SIGN the following statement with your exam:

I certify that I have neither given nor received any assistance on this exam and have used no resources other than those allowed.

Exams submitted without this certification WILL NOT BE GRADED.

Since my mathematical youth, I have been under the spell of the classical theory of Galois. This charm has forced me to return to it again and again.

Mario Livio

Since the art [of algebra] surpasses all human subtlety... and is truly a celestial gift and a very clear test of the capacity of man's minds, whoever applies himself to it will believe that there is nothing that he cannot understand.

Gerolamo Cardano

Beware the mathematician and others who make false prophecies. The danger already exists that the mathematicians have made a pact with the Devil to darken the spirit and confine Man within the bonds of Hell.

St. Augustine (who was technically talking about astrologers, but nonetheless had the correct sentiment)

---

1. [55] (The A-Zs of Algebra) Calculate the following (please justify your responses, but each response only needs to be a few sentences):

   (a) Whether or not $\mathbb{F}_7[x]$ modulo $x^3 + x + 1$ is a field.

   (b) The multiplicative inverse of $3 + \sqrt[3]{2}$ inside $\mathbb{Q}(\sqrt[3]{2})$, in the form $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ for $a, b, c \in \mathbb{Q}$.

   (c) The degree of the field extension $\mathbb{F}_{2^{20}}/\mathbb{F}_{2^5}$.

   (d) The degree of the splitting field of $x^7 - 7$ over $\mathbb{Q}$.

   (e) A basis for the splitting field of $x^3 - 3$ over $\mathbb{Q}$.

   (f) An element of order exactly 6 inside $(\mathbb{Z}/31\mathbb{Z})^\times$.

   (g) The subgroup diagram of $\mathbb{Z}/40\mathbb{Z}$.

   (h) Find the orbit and the stabilizer of the element $p = x_1x_3 + x_2x_4$ under the action of S_4 on polynomials $F[x_1, x_2, x_3, x_4]$.

   (i) The number of conjugacy classes of elements in S_6.

   (j) All of the abelian groups of order 200, up to isomorphism.

   (k) The number of Sylow 5-subgroups of S_7.

   (l) Three mutually non-isomorphic groups of order 28.

   (m) The subfield diagram of $\mathbb{Q}(5^{1/3}, \zeta_3)/\mathbb{Q}$.

   (n) The degree of the minimal polynomial of $\sqrt{2} + \sqrt[3]{5}$ over $\mathbb{Q}$.

   (o) The minimal polynomial of $2^{1/4} + i$ over $\mathbb{Q}$ (it can be left factored) and its Galois group.

   (p) The number of monic irreducible polynomials of degree 6 over $\mathbb{F}_7$.

   (q) A generator of the subfield of $\mathbb{Q}(\zeta_{17})/\mathbb{Q}$ that has degree 4 over $\mathbb{Q}$.

   (r) Whether a regular 2020-gon or regular 2040-gon can be constructed with straightedge and compass.

   (s) The Galois group of $\mathbb{Q}(\zeta_{51})/\mathbb{Q}$, as a direct product of cyclic groups.

   (t) The Galois group of $f(y) = y^3 + 3y + 6$ over $\mathbb{Q}$.

   (u) The Galois group of $f(y) = y^3 - 3y - 1$ over $\mathbb{Q}$.

   (v) The Galois group of $f(y) = y^4 + 3y - 3$ over $\mathbb{Q}$.

   (w) The Galois group of $f(y) = y^4 + 3y + 3$ over $\mathbb{Q}$.

   (x) The Galois group of $f(y) = y^5 - 8y + 6$ over $\mathbb{Q}$. [Hint: Count real roots.]

   (y) The factorization structure for $f(t) = x^5 - 5x^3 + 5x - 5$ modulo p for the 100 smallest primes not dividing its discriminant is given below. Find the most probable Galois group for f over $\mathbb{Q}$, and determine (based on that identification) whether f is solvable in radicals.

Factorization Type	1	2,2	4	5
# Appearances	3	22	52	23

   (z) The factorization structure for $f(t) = x^7 - 2x^6 + 2x + 2$ modulo p for the 100 smallest primes not dividing its discriminant is given below. Find the most probable Galois group for f over $\mathbb{Q}$, and determine (based on that identification) whether f is solvable in radicals.

Factorization Type	2,2	2,2,3	2,4	3	3,3	5	7
# Appearances	2	7	21	2	9	23	36

---

2. [5] Suppose K/F is an algebraic extension of fields and R is a subring of the field K that contains F. Prove that R is in fact a field.

---

3. [5] Let G be a group of order n. Prove that G is isomorphic to a subgroup of the alternating group A_{n+2}.

---

4. [10] The goal of this problem is to prove that there is no simple group of order 11830. So suppose G is simple of order $11830 = 2 \cdot 5 \cdot 7 \cdot 13^2$.

   (a) Show that the Sylow numbers n_7 and n_{13} of G must equal 169 and 14, respectively.

   (b) Show that G contains a subgroup H of index 14. Deduce that G would be isomorphic to a subgroup of S_{14} and obtain a contradiction. [Hint: Use Sylow's theorems and $n_{13} = 14$, and then consider the left-multiplication action of G on H.]

---

5. [10] Let $f(y) = y^6 - 2$.

   (a) Show that the splitting field of f over $\mathbb{Q}$ is $K = \mathbb{Q}(2^{1/6}, \zeta_6)$, and show that $[K : \mathbb{Q}] = 12$.

   (b) Find the Galois group of f over $\mathbb{Q}$.

---

6. [5] Suppose $f(x) \in \mathbb{Q}[x]$ has degree 4 and Galois group A_4. If α is any root of f, show that $\mathbb{Q}(\alpha)$ is a degree-4 extension of $\mathbb{Q}$ that contains no subfield E with $[E : \mathbb{Q}] = 2$. [Hint: A_4 has no subgroup of index 2.]

---

7. [10] Let $f(y) = y^6 + 9y^4 - 14y^3 + 27y^2 + 126y + 76$. Let K be the splitting field of f over $\mathbb{Q}$, and observe (you do NOT need to verify this calculation!) that one root of f in K is $\alpha = \sqrt[3]{7} + \sqrt{-3}$.

   (a) Determine the other roots of f. [Hint: Compute the Galois conjugates of α inside $\mathbb{Q}(7^{1/3}, \zeta_3)$.]

   (b) Show that $K = \mathbb{Q}(\alpha)$ and that f is irreducible. Conclude that the other five roots of f are rational polynomials in α.

   (c) Determine the Galois group of f, and show that $f(y)$ is reducible modulo p for every prime p. [Hint: Consult entry 6T2 of the transitive subgroup tables.]
