
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 12 problems on this exam, with points as indicated.

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.

It is not knowledge, but the act of learning, not possession but the act of getting there, which grants the greatest enjoyment.

Carl Friedrich Gauss

In real life, I assure you, there is no such thing as algebra.

Fran Lebowitz

Friggatriskaidekaphobia, *n.* or paraskavedekatriaphobia, *n.*: The fear of Friday the 13th.

A dictionary

---

1. (5) Suppose p is a prime, and n and i are any positive integers with $0 \leq i \leq n$. Prove that $\binom{pn}{pi} \equiv \binom{n}{i} \bmod p$. [Hint: Show $(1+x)^{pn} = (1+x^p)^n$ over $\mathbb{F}_p$.]

---

2. (5) Construct explicitly a field with exactly $343 = 7^3$ elements. Make sure to justify why it is a field.

---

3. (5) Prove that there do not exist rational numbers a, b, c such that $\sqrt[7]{2} = a + \sqrt{b} + \sqrt[3]{c}$.

---

4. (5) Suppose K/F is a field extension and that $[K:F] = p$ is a prime number. Prove that $K = F(\alpha)$ for any element $\alpha \in K$ that is not in F.

---

5. (15) Let $q(x) = x^4 - 3$ and $r(x) = x^{12} - 27$ over $\mathbb{Q}$, and take K to be the splitting field of $q(x)$ over $\mathbb{Q}$.

   (a) Show that $K = \mathbb{Q}(3^{1/4}, i)$ and determine $[K:\mathbb{Q}]$.

   (b) Show that $q(x)$ is irreducible over $\mathbb{Q}(i)$.

   (c) Show that every root of $r(x)$ lies in K, and that K is also the splitting field of $r(x)$ over $\mathbb{Q}$.

---

6. (15) Let K/F be a field extension and $\alpha \in K$. The goal of this problem is to study the relationship between $F(\alpha)$ and $F(\alpha^2)$.

   (a) Show that $F(\alpha)/F(\alpha^2)$ is an extension of degree 1 or 2.

   (b) If $F(\alpha) = F(\alpha^2)$ show that α must be algebraic over F. Conclude that if α is transcendental over F, then $[F(\alpha):F(\alpha^2)] = 2$.

   (c) Suppose that α is algebraic over F and the minimal polynomial $m(x)$ for α over F has a term of odd degree (i.e., a term of the form $a_d x^d$ with $a_d \neq 0$ and d odd). Show that $F(\alpha) = F(\alpha^2)$. [Hint: Solve for α explicitly as a rational function of α^2.]

   (d) Inversely, suppose α is algebraic over F and its minimal polynomial only has even-degree terms. Show that $[F(\alpha):F(\alpha^2)] = 2$. [Hint: Find a polynomial of which α^2 is a root and consider its degree.]

---

7. (15) Let p be an odd prime and set $\zeta_p = e^{2\pi i/p}$ as usual, with $K = \mathbb{Q}(\zeta_p)$.

   (a) Show that $F = \mathbb{Q}(\cos(2\pi/p))$ is a subfield of K. [Hint: Compute $\zeta_p + \zeta_p^{-1}$.]

   (b) Show that ζ_p is algebraic of degree 2 over F, and deduce that $[K:F] = 2$.

   (c) Show that $\cos(2\pi/p)$ is algebraic over $\mathbb{Q}$ of degree $(p-1)/2$.

   (d) Prove that if the regular p-gon is constructible with straightedge and compass, then $p = 2^{2^n} + 1$ for some integer n. [Hint: Show that if $p = 2^k + 1$ is prime, then k must be a power of 2.]

---

8. (5) Find a counterexample to the following statement: "If G_1 and G_2 are groups, then every subgroup of $G_1 \times G_2$ is of the form $H_1 \times H_2$ where H_1 is a subgroup of G_1 and H_2 is a subgroup of G_2".

---

9. (5) Let G be a group. Show that the map $\varphi : G \to G$ defined by $\varphi(g) = g^{-1}$ is a group homomorphism if and only if G is abelian.

---

10. (5) Recall that $GL_n(\mathbb{F}_p)$ is the group of invertible $n \times n$ matrices with entries from $\mathbb{F}_p$, and $SL_n(\mathbb{F}_p)$ is the subgroup of determinant-1 matrices. Show that $SL_n(\mathbb{F}_p)$ is a normal subgroup of $GL_n(\mathbb{F}_p)$ and that the quotient is isomorphic to $\mathbb{F}_p^\times$. [Hint: Use the determinant map $\varphi : GL_n(\mathbb{F}_p) \to \mathbb{F}_p^\times$.]

---

11. (10) Let $n \geq 2$ be a positive integer.

    (a) Show that S_n is generated by transpositions.

    (b) Show that S_n is generated by the transpositions $(1\,2)$, $(1\,3)$, $(1\,4)$, ... , $(1\,n)$.

    (c) Show that S_n is generated by $(1\,2)$ and $(2\,3\,\ldots\,n)$.

---

12. (10) Let n be a positive integer.

    (a) Show that S_8 has a subgroup isomorphic to the quaternion group Q_8.

    (b) Show that S_n does not have a subgroup isomorphic to Q_8 for any $n \leq 7$. [Hint: If Q_8 acts on a set with ≤ 7 elements, use the orbit-stabilizer theorem to show that the stabilizer of any point must contain -1.]

    (c) Find, with justification, the smallest n such that S_n has a subgroup isomorphic to the dihedral group $D_{2\cdot 7}$.
