

Final Exam: Math 100C, Spring 2023

You have 3 hours

You are not permitted to use calculators, books, or notes.

YOU MUST SHOW ALL YOUR WORK TO RECEIVE CREDIT.

Name _____

“I have adhered to UCSD policies on academic integrity while completing this examination.”

Signature _____

There are 10 problems; each problem is worth 20 points.

Good luck!

Problem 1. (20 points) Answer TRUE if the statement is true, and FALSE if the statement is false. For this question, you do not need to show your work or justify your response.

1. (5 points) The ring $\mathbf{Z}[x, y, z]/(y^2 - xz)$ is Noetherian.
This is TRUE

2. (5 points) Suppose n is a positive integer and $M \subseteq \mathbf{Z}^n$ is a subgroup. Then there exists n elements $m_1, \dots, m_n$ of M so that M is generated by $m_1, \dots, m_n$, i.e., $M = \mathbf{Z}m_1 + \dots + \mathbf{Z}m_n$.
This is TRUE

3. (5 points) Let C_n denote the cyclic group of order n . Then $C_2 \times C_4 \times C_8$ is isomorphic to $C_4 \times C_{16}$.
This is FALSE

4. (5 points) Suppose F is a field and V is a 10-dimensional F vector space. Let $N : V \rightarrow V$ be a linear map that satisfies $N^{100} = 0$. Then necessarily $N^{10} = 0$.
This is TRUE

Problem 2. (20 points) For a prime power q , let $\mathbf{F}_q$ denote the field of order q .

1. (10 points) How many subfields does $\mathbf{F}_{2^6}$ have?

Proof. There is one subfield for each positive integer divisor of 6 (1, 2, 3, 6). Thus there are 4 subfields. $\square$

2. (10 points) How many **primitive elements** does $\mathbf{F}_{2^6}$ have?

Proof. A primitive element is one which is not in any subfield. There are 2 elements in $\mathbf{F}_2$, 4 elements in $\mathbf{F}_{2^2}$, 8 elements in $\mathbf{F}_{2^3}$. The intersection of $\mathbf{F}_{2^2}$ and $\mathbf{F}_{2^3}$ is $\mathbf{F}_2$. Thus there are a total of $4 + 8 - 2 = 10$ elements of $\mathbf{F}_{2^6}$ that are **not** primitive. Hence there are $54 = 2^6 - 10$ elements that are primitive. $\square$

Problem 3. (20 points) Suppose $f(x) \in \mathbf{Q}[x]$ is a monic irreducible polynomial. Assume in $\mathbf{C}[x]$ the polynomial f factors as $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$, and let $E \subseteq \mathbf{C}$ be the splitting field of $f(x)$ in $\mathbf{C}$.

1. (10 points) Recall that $D(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$ is called the discriminant of the polynomial f . Explain how one knows that $D(f) \in \mathbf{Q}$.

Proof. There are a few ways to do this. One way is to use symmetric polynomials: The discriminant is a symmetric polynomial in the α_j , and so can be expressed as a polynomial in the s_j with integer coefficients, where s_j are the elementary symmetric polynomials in the α_k . But the s_j are the coefficients of the polynomial f , so are rational numbers. $\square$

2. (10 points) Let $G = \text{Gal}(E/\mathbf{Q})$, and suppose $D(f)$ is a square in $\mathbf{Q}$, i.e., there exists $\delta \in \mathbf{Q}$ so that $D(f) = \delta^2$. Explain how one knows that in this case, the Galois group G is isomorphic to a subgroup of the alternating group $A_n \subseteq S_n$.

Proof. We have $\prod_{i < j} (\alpha_i - \alpha_j) = \pm \delta$, so is in $\mathbf{Q}$. The action of G on the roots α_i defines an embedding $G \hookrightarrow S_n$. If $\sigma \in S_n$, then $\sigma(\prod_{i < j} (\alpha_i - \alpha_j)) = \text{sgn}(\sigma) \prod_{i < j} (\alpha_i - \alpha_j)$. Thus if $\sigma \in G$, $\sigma(\delta) = \delta$, so $\text{sgn}(\sigma) = 1$. Consequently, the embedding of $G \hookrightarrow S_n$ lands in the alternating group A_n .

Although it is not required for full credit, here is how one can easily check that $\sigma(\prod_{i < j} (\alpha_i - \alpha_j)) = \text{sgn}(\sigma) \prod_{i < j} (\alpha_i - \alpha_j)$. One observes that because $D(f)$ is S_n invariant, we must have $\sigma(\prod_{i < j} (\alpha_i - \alpha_j)) = \epsilon(\sigma) \prod_{i < j} (\alpha_i - \alpha_j)$ for some $\epsilon : S_n \rightarrow \pm 1$. It is clear that ϵ is a group homomorphism, so either ϵ is trivial or is the sign character. To see that ϵ is the sign character, we must only evaluate $\epsilon((12))$. In this special case, it is easy to see $\epsilon((12)) = -1$, finishing the proof. $\square$

The above problem was from discussion section.

Problem 4. (20 points) Let $E = \mathbf{Q}(i, 2^{1/4}) \subseteq \mathbf{C}$. Observe that, because $i \notin \mathbf{Q}(2^{1/4})$, $[E : \mathbf{Q}] = 8$ and then $[E : \mathbf{Q}(i)] = 4$. (You may use these facts without reproving them.)

1. (5 points) Prove that $\text{Gal}(E/\mathbf{Q}(i))$ is cyclic of order four.

Proof. E is a splitting field of $x^4 - 2$, so is Galois over $\mathbf{Q}$ and Galois over any of its subfields, such as $\mathbf{Q}(i)$. We thus know $\text{Gal}(E/\mathbf{Q}(i))$ has order 4, and it remains to show that it is cyclic. But this comes from Kummer theory. Specifically, the map $\text{Gal}(E/\mathbf{Q}(i)) \rightarrow C_4 \simeq \{1, i, -1, -i\}$ given by $g \mapsto g(2^{1/4})/2^{1/4}$ is an injective group homomorphism, so $\text{Gal}(E/\mathbf{Q}(i))$ is cyclic. $\square$

2. (15 points) Prove that $\text{Gal}(E/\mathbf{Q})$ is dihedral of order 8. **For this part of the problem, you may assume the prior part, even if you did not answer the prior part.**

Proof. Let $G = \text{Gal}(E/\mathbf{Q})$. We already know: G has a normal subgroup $C = \text{Gal}(E/\mathbf{Q}(i))$ that is cyclic of order 4, and such that $G/C \simeq C_2 = \text{Gal}(\mathbf{Q}(i)/\mathbf{Q})$. Moreover, this C_2 lifts to a subgroup of G as $\text{Gal}(E/\mathbf{Q}(2^{1/4}))$. It follows that $G \simeq C_4 \rtimes C_2$. To prove that G is isomorphic to the dihedral group of order 8, we must compute the conjugation action of the C_2 on the C_4 . Thus suppose $g \in C_4$, and $g(2^{1/4}) = \zeta 2^{1/4}$, with $\zeta \in \mu_4$. If c denotes complex conjugation, then clearly $(cgc^{-1})(2^{1/4}) = \bar{\zeta} 2^{1/4}$. Because the identification of C with C_4 is through the roots of unity μ_4 , this equation proves the desired conjugation action. $\square$

The above problem was from discussion section.

Problem 5. (20 points) Let F be a field, V a four-dimensional F vector space, and $T : V \rightarrow V$ a linear operator. Is it possible that there exists a cubic irreducible polynomial $f(x) \in F[x]$ so that $f(T) = 0$ on V ? Be sure to justify your response.

Proof. No, it is not possible that such an f exists. Indeed, set $E = F[x]/(f(x))$, a cubic field extension of F . If $f(T) = 0$ on V , then V is a finitely generated module for E , i.e., V has the structure of an E -vector space. But then $V \approx E^k$ for some k , so $\dim_F(V) = 3k$ is divisible by 3, a contradiction. $\square$

The above problem is a special case of a problem on the review worksheet for the final exam.

Problem 6. (20 points) Let G denote the abelian group with generators x, y , subject to the relations $x^{100} = 1$, $y^{50} = 1$ and $x^{25} = y^{25}$. Write G as a product of cyclic groups. Be sure to prove your answer.

Proof. A presentation matrix for G is $A = \begin{pmatrix} 100 & 0 & 25 \\ 0 & 50 & -25 \end{pmatrix}$. Using row and column operations, one obtains the matrix $A' = \begin{pmatrix} 0 & 50 & 0 \\ 0 & 0 & 25 \end{pmatrix}$. Thus $G \simeq C_{50} \times C_{25}$.

□

This problem is very similar to one on the review worksheet for the final exam.

Problem 7. (20 points) Suppose E_1 and E_2 are Galois extensions of $\mathbf{Q}$ in $\mathbf{C}$ with $\text{Gal}(E_1/\mathbf{Q}) \simeq \text{Gal}(E_2/\mathbf{Q}) \simeq S_3$. Let $K = E_1 \cap E_2$ and assume that K is quadratic over $\mathbf{Q}$. Let E denote the compositum of E_1 and E_2 in $\mathbf{C}$. How many subfields of E are there that contain K ? Be sure to prove your answer.

Proof. The map $S_3 = \text{Gal}(E_j/\mathbf{Q}) \rightarrow \text{Gal}(K/\mathbf{Q}) = C_2$ is the sign map. By our theorems on the Galois groups of composite extensions, E/K is Galois with $\text{Gal}(E/K) \simeq A_3 \times A_3$. This group has 4 subgroups, so there are four subfields of E that contain K . $\square$

This problem is very similar to one from review sheet 2.

Problem 8. (20 points) Suppose $K/\mathbf{Q}$ is a Galois extension of degree three. Let $F = \mathbf{Q}(\mu_3)$. We consider both K and F as subfields of $\mathbf{C}$. Let L denote the compositum of K and F in $\mathbf{C}$.

For each part of this problem, you may assume the prior parts, even if you did not answer the prior parts.

1. (5 points) Prove that $L/\mathbf{Q}$ is Galois, and $\text{Gal}(L/\mathbf{Q}) \simeq C_3 \times C_2$. Here C_n denotes the cyclic group of order n .

Proof. Because $\gcd(2, 3) = 1$, $K \cap F = \mathbf{Q}$ so our theorems on Galois groups of composite extensions imply $\text{Gal}(L/\mathbf{Q}) \simeq C_3 \times C_2$. □

2. (5 points) Prove that there exists $v \in F^\times$ so that $L = F(v^{1/3})$.

Proof. F contains μ_3 , and $\text{Gal}(L/F)$ is cyclic of degree 3, so this follows from Kummer theory. □

3. (10 points) With v as in the previous part, let $\bar{v}$ denote the complex conjugate of v . Prove that $\bar{v} \equiv v^2 \pmod{(F^\times)^3}$, i.e., that there exists $w \in F^\times$ so that $\bar{v} = v^2 w^3$.

Proof. Let c denote complex conjugation. If $\sigma \in \text{Gal}(L/F)$, then $c\sigma = \sigma c$ on L by part (1) of the problem. Consequently,

$$\sigma(\bar{v}^{1/3}) = c\sigma(v^{1/3}) = c(\zeta v^{1/3}) = \zeta^2 \bar{v}^{1/3}$$

because $\bar{\zeta} = \zeta^2$ for $\zeta \in \mu_3$. But $\sigma(v^{2/3}) = \zeta^2 v^{2/3}$. Thus $\bar{v}^{1/3} v^{-2/3}$ is fixed by $\text{Gal}(L/F)$, so is in $F^\times$. Cubing gives the desired relation. □

This problem was on the review sheet for Exam 2.

Problem 9. (20 points) Let $n \geq 3$ be an integer and let D_n denote the dihedral group of order $2n$. Prove that every irreducible representation of D_n has dimension 1 or 2.

Proof. We have $C_n \subseteq D_n$ is abelian, and normal of index 2. Let V be the space of an irrep of D_n . Then C_n has a nonzero eigenvector on V , say v . Let $\sigma \in D_n \setminus C_n$, and set $w = \sigma(v)$. One verifies immediately that $\mathbf{C}v + \mathbf{C}w$ is stable by both σ and C_n , using that C_n is normal. Thus $\dim(V) \leq 2$. $\square$

This problem is a special case of a problem on the review worksheet for the final exam.

Problem 10. (20 points) Let C_4 denote the cyclic group of order 4 and let K_4 denote the Klein 4-group.

1. (10 points) Make a character table for C_4 .

Proof. Of course, the tables you come up with depend upon exactly how you order the elements of these groups and the irreps. Here is one possibility.

*	$0 + 4\mathbf{Z}$	$1 + 4\mathbf{Z}$	$2 + 4\mathbf{Z}$	$3 + 4\mathbf{Z}$
χ_1	1	1	1	1
χ_2	1	i	-1	$-i$
χ_3	1	-1	1	-1
χ_4	1	$-i$	-1	i

□

2. (10 points) Make a character table for K_4 .

Proof.

*	$(1, 1)$	$(1, -1)$	$(-1, 1)$	$(-1, -1)$
χ_1	1	1	1	1
χ_2	1	1	-1	-1
χ_3	1	-1	1	-1
χ_4	1	-1	-1	1

□

This problem was on the review worksheet for the final exam.

THIS PAGE INTENTIONALLY LEFT BLANK