

Exam 1: Math 100C, Spring 2023

You have 50 minutes.

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 5 problems; each problem is worth 20 points.

Good luck!

Problem 1. (20 points) Let p be a prime number. Give a simple formula in terms of p for the number of elements in the group $\text{GL}_3(\mathbf{F}_p)$. Be sure to prove your answer.

Proof. This is a special case of a discussion section question. There are $p^3 - 1$ possibilities for the first column (everything but 0), $p^3 - p$ possibilities for the second column (everything but a multiple of the first column), and $p^3 - p^2$ possibilities for the third column (everything that is not in the span of the first two columns.) This leaves $(p^3 - 1)(p^3 - p)(p^3 - p^2)$ elements in $\text{GL}_3(\mathbf{F}_p)$.

□

Problem 2. (20 points) Suppose n is a positive integer and p is a prime number which is relatively prime to n . Assume $f(x) \in \mathbf{Z}[x]$ is a monic polynomial of positive degree that divides the polynomial $x^n - 1$ in $\mathbf{Z}[x]$, i.e., there exists a polynomial $g(x) \in \mathbf{Z}[x]$ so that $x^n - 1 = f(x)g(x)$. Prove that the mod p reduction of $f(x)$ has no multiple roots in any field of characteristic p .

Proof. One way to do this problem is to use the derivative test, and was on the practice worksheet for exam 1. Because $f(x)$ divides $x^n - 1$, it suffices to check that $x^n - 1$ does not have multiple roots in a field of characteristic p . For this, it is sufficient to check that $x^n - 1$ is relatively prime to its derivative nx^{n-1} over $\mathbf{F}_p$. But we have $x(nx^{n-1}) - n(x^n - 1) = n \in \mathbf{F}_p^\times$, because $(n, p) = 1$. This proves the claim.

Here is an alternate proof. Suppose for the sake of contradiction that α is a multiple root of $x^n - 1$ in some field L of characteristic p . Then $\alpha^n - 1 = 0$ and $n\alpha^{n-1} = 0$. But the second equation implies $\alpha = 0$, because $(n, p) = 1$, which contradicts the first equation. $\square$

Problem 3. (20 points) For this question, answer *TRUE* if the statement is true, and *FALSE* if the statement is false. For this question only, you do not need to show your work or provide an explanation.

1. (5 points) There exists a monic irreducible polynomial $f(x) \in \mathbf{Q}[x]$ of degree 11 which becomes reducible over $\mathbf{Q}[\sqrt{3}]$.

Proof. This is FALSE. It is a special case of a homework question from HW2. □

2. (5 points) For every positive integer n , there exists a monic irreducible polynomial in $\mathbf{F}_{11}[x]$ of degree n .

Proof. This is TRUE. This is from class. One takes the minimal polynomial for a primitive element of $\mathbf{F}_{11^n}$ over $\mathbf{F}_{11}$. (Of course, there is nothing special about 11 here, it is true for every p). □

3. (5 points) Set $K = \mathbf{F}_{81}$ and $F = \mathbf{F}_3$. If an element $\gamma \in K$ is a primitive element for the extension K/F , then γ necessarily generates the multiplicative group $K^\times$.

Proof. This is FALSE. You found a counterexample on HW2. □

4. (5 points) Suppose $n_1, n_2 \in \mathbf{Z}$ are distinct square-free integers, neither of which is equal to 1. Then $\mathbf{Q}(\sqrt{n_1})$ cannot be isomorphic to $\mathbf{Q}(\sqrt{n_2})$ as fields.

Proof. This is TRUE. This is from HW1. □

Problem 4. (20 points) Let $p = 3$ and $r = 12$. How many subfields does $K = \mathbf{F}_{p^r} = \mathbf{F}_{3^{12}}$ contain? Be sure to justify your answer.

Proof. This is from class and HW2. The subfields of K are exactly the $\mathbf{F}_{p^k}$ with $k|r$ (and each appears in K with multiplicity one.) Thus there are 6 subfields of K , corresponding to the 6 divisors of 12: 1, 2, 3, 4, 6, 12.

□

Problem 5. (20 points) Give an example of a field extension $K/\mathbf{Q}$ so that the degree $[K : \mathbf{Q}] = 5$ but $\text{Aut}(K/\mathbf{Q}) = \{1\}$. Be sure to justify your answer.

Proof. This is just like an example from class. For instance, we could take $K = \mathbf{Q}(2^{1/5})$. The polynomial $x^5 - 2$ is irreducible (by Eisenstein) so K has degree 5 over $\mathbf{Q}$. However, the other roots of $x^5 - 2$ are $\zeta_5^a 2^{1/5}$, $a \in \{1, 2, 3, 4\}$, where $\zeta_5 = e^{2\pi i/5}$. None of these other roots are real, so in particular they are not in K . Thus $\text{Aut}(K/\mathbf{Q}) = \{1\}$. (Every automorphism of K over $\mathbf{Q}$ must send $2^{1/5}$ to a root of this polynomial. Alternatively, if $K = F(\gamma)$, and γ has irreducible polynomial $f(x) \in F[x]$, then we proved that $\text{Aut}(K/F)$ has size the number of roots of $f(x)$ in K .) $\square$

THIS PAGE INTENTIONALLY LEFT BLANK