Exam 2: Math 100C, Spring 2024

You have 60 minutes.

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

YOU MUST SHOW ALL YOUR WORK TO RECEIVE CREDIT,
(unless a problem specifies otherwise)

Name _____

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

Signature _____

There are 5 regular problems, worth 20 points each, and one bonus problem, worth 10 points.

Good luck!

Problem 1. *(20 points) Recall that you proved on a homework question that if $a, b \in \mathbf{Q}^\times$ with $a \notin (\mathbf{Q}^\times)^2, b \notin (\mathbf{Q}^\times)^2$ and $ab \notin (\mathbf{Q}^\times)^2$, then $\mathbf{Q}(\sqrt{a}, \sqrt{b})$ is Galois over $\mathbf{Q}$ with Galois group isomorphic to the Klein four group. Suppose $\gamma = w + x\sqrt{a} + y\sqrt{b} + z\sqrt{ab}$, with $w, x, y, z \in \mathbf{Q}$. Write down explicitly (in terms of a, b, w, x, y, z) the four elements $\sigma(\gamma)$ where σ ranges over elements of $Gal(\mathbf{Q}(\sqrt{a}, \sqrt{b})/\mathbf{Q})$. You do not need to justify your answer for this question.*

Proof. The four elements $\sigma(\gamma)$ are

1. $w + x\sqrt{a} + y\sqrt{b} + z\sqrt{ab}$
2. $w - x\sqrt{a} + y\sqrt{b} - z\sqrt{ab}$
3. $w + x\sqrt{a} - y\sqrt{b} - z\sqrt{ab}$
4. $w - x\sqrt{a} - y\sqrt{b} + z\sqrt{ab}$

□

Problem 2. *(20 points) For a positive integer n, let $\zeta_n = e^{2\pi i/n}$. Prove that $2^{1/3}$ is not contained in $\mathbf{Q}(\zeta_n)$ for any n.* ***Hint****: We proved in class that $Gal(\mathbf{Q}(\zeta_n)/\mathbf{Q})$ is abelian. You may use this fact.*

Proof. There are at least two (similar) ways to do this problem, using that $\mathbf{Q}(\zeta_n)$ is Galois over $\mathbf{Q}$ with abelian Galois group.

1. Way 1: Set $K = \mathbf{Q}(\zeta_n)$. Let L be an arbitrary intermediate field, $K \supseteq L \supseteq \mathbf{Q}$ and let $H = Gal(K/L)$. Because $Gal(K/\mathbf{Q})$ is abelian, H is a normal subgroup of $Gal(K/\mathbf{Q})$, and thus L is Galois over $\mathbf{Q}$. Consequently, if $2^{1/3} \in K$, then $L = \mathbf{Q}(2^{1/3})$ would have to be Galois over $\mathbf{Q}$, a contradiction. (The other roots of $x^3 - 2$ are not in L, which is a subfield of $\mathbf{R}$.)
2. Way 2: Again, let $K = \mathbf{Q}(\zeta_n)$. Suppose $2^{1/3} \in K$. Then by the Splitting Theorem, $x^3 - 2$ would split completely in K, so $L = \mathbf{Q}(2^{1/3}, e^{2\pi i/3})$ would be a subfield of K. But then L is Galois over $\mathbf{Q}$, so $Gal(K/\mathbf{Q})$ would have to surject onto $Gal(L/\mathbf{Q})$. The latter group is S_3 and the former is abelian, a contradiction (because any quotient of an abelian group is again abelian.)

□

Problem 3. *(20 points) Suppose F is a field of characteristic 0, and K is a finite Galois extension of F, with $Gal(K/F) = G$. If $\alpha \in K$, set $N(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$, the product over the elements $\sigma(\alpha)$ of K, as σ ranges over $G = Gal(K/F)$. Prove that $N(\alpha) \in F$ for all $\alpha \in K$.* ***Hint****: Recall that $K^G = F$.*

Proof. One simply observes that if $g \in G$, then g permutes the elements $\sigma(\alpha)$ as σ ranges over elements of G. Thus $N(\alpha)$ is fixed by g for every $g \in G$. Consequently, $N(\alpha) \in K^G = F$. □

Problem 4. *(20 points) Let p be a prime number, and suppose F is a finite field of characteristic p. Suppose $f(x) = a_n x^{np} + a_{n-1}x^{(n-1)p} + a_{n-2}x^{(n-2)p} + \cdots + a_1 x^p + a_0 \in F[x]$. Note that the coefficient of x^r in $f(x)$ is 0 unless r is a multiple of p. Prove that there exists a polynomial $g(x) \in F[x]$ so that $f(x) = (g(x))^p$.*

Proof. Let φ be the Frobenius automorphism of F. Then $\varphi : F \to F$ is surjective; this was proved on a homework. (The one line proof of this fact is that φ is immediately checked to be injective, because F is a field, and thus must also be surjective, because F is finite.) Consequently, for each a_n, there exits $b_n \in F$ with $b_n^p = a_n$. Concretely, if F has size p^r, then $b_n = a_n^{p^{r-1}}$.

Now set $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$. Because $(u+v)^p = u^p + v^p$ in rings of characteristic p, $g(x)^p = f(x)$. □

Problem 5. *(20 points) Write TRUE if the statement is true, and write FALSE if the statement is false. For this question, you do not need to justify your response.*

1. *(5 points) Suppose F is a field of characteristic 0, and $f(x) \in F[x]$ is an irreducible monic polynomial of degree 3. Let K denote a splitting field of f. Then $Gal(K/F)$ is cyclic of order 3 if and only if the discriminant of $f(x)$ is in $(F^\times)^2$.*
   TRUE. We proved this in class.

2. *(5 points) Suppose $K \supseteq L \supseteq F$ are a tower of fields of characteristic 0. If K/L is Galois and L/F is Galois then necessarily K/F is Galois.*
   FALSE.

3. *(5 points) Suppose F_1, F_2 are finite fields of size 27. Then there is exactly one isomorphism of fields $\varphi : F_1 \to F_2$.*
   FALSE. The fields F_1 and F_2 are isomorphic, so such a φ exists. But if φ is one such isomorphism, then $\sigma \circ \varphi$ is a genuinely different one, where σ is the Frobenius of F_2. Thus there is not exactly one. (In fact ,there are three isomorphisms, as you can check.)

4. *(5 points) Suppose F is a field of characteristic 0, and K is a finite Galois extension of F. Let L be an intermediate field of the extension K/F, so that $K \supseteq L \supseteq F$. Then necessarily K is Galois over L.*
   TRUE. This is one of the parts of the main theorem of Galois theory.

Problem 6. ***Bonus*** *(10 points) Given an example of a subfield K of $\mathbf{C}$ so that $K/\mathbf{Q}$ is a finite Galois extension, with $Gal(K/\mathbf{Q})$ cyclic of order 8.*

Proof. Let $E = \mathbf{Q}(\zeta_{17})$ and $K = \mathbf{Q}(\zeta_{17} + \zeta_{17}^{-1})$. Then $E/\mathbf{Q}$ is Galois with Galois group $(\mathbf{Z}/17\mathbf{Z})^{\times}$. This group is cyclic of order 16, as we proved when we discussed finite fields. It is not difficult to see that E/K is a quadratic extension: ζ_{17} satisfies a quadratic polynomial over K, so the degree $[E : K]$ is at most two. It is at least two because E is genuinely complex while K is a subfield of $\mathbf{R}$. Thus $Gal(K/\mathbf{Q})$ is quotient of C_{16} (the cyclic group of order 16), by a subgroup of order 2. So, it is cyclic of order 8. □

THIS PAGE INTENTIONALLY LEFT BLANK