Math 422/501 Final - Dec 15, 2016

Name:

ID number:

- The test consists of **six questions** on **eight pages**.
- No calculators or notes or books allowed.
- If you need more space for a problem, continue on the back of the page or on a separate paper. But **label clearly** that your answer continues somewhere else.
- You can use (without proof) any statement we've proven in class or on the homework. If you're unsure whether something counts, ask me.

Problem 1 - True/False. For each of the following statements, write whether it is true or false and *justify your answer* by either citing theorems or providing a (counter)example.

(a) There is a finite inseparable extension $K/\mathbb{F}_q$ for some finite field $\mathbb{F}_q$.

(b) There is a field K with no irreducible polynomials of degree 3 in $K[x]$.

(c) If $K/\mathbb{Q}$ is the splitting field of an irreducible quartic, and $\mathrm{Gal}(K/\mathbb{Q}) \cong S_4$, then K is also the splitting field of an irreducible polynomial of degree 24.

Problem 1 - Continued.

(d) If K is a field and $G \subseteq \mathrm{Aut}(K)$ is a finite group of automorphisms, $[K : K^G]$ is always equal to $|G|$.

(e) There is an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ satisfying $f(\sqrt{2}) = f(\sqrt{3}) = 0$.

Problem 2. (a) Factor the polynomial $x^4+x^2+1 \in \mathbb{F}_2[x]$ into irreducibles (and justify they are irreducible).

(b) Factor the polynomial $x^4 - x^3 - x^2 - x - 1 \in \mathbb{F}_3[x]$ into irreducibles (and justify they are irreducible).

(c) Justify that $x^4 + 2x^3 - x^2 + 2x + 1 \in \mathbb{Q}[x]$ is irreducible. (Hint: There is a reason this is after parts (a) and (b)).

Problem 3. Find a Galois extension $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong Z_3 \times Z_3 \times Z_3$ as a subfield of a cyclotomic field $\mathbb{Q}(\zeta_n)$, by coming up with a specific integer n and explaining how you can construct a subgroup $H \leq \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ such that the fixed field $K = \mathbb{Q}(\zeta_n)^H$ works.

Problem 4. Recall the *quaternion group* Q_8 is the finite group with eight elements ± 1, $\pm i$, $\pm j$, $\pm k$ with multiplication defined by having 1 and -1 do what you'd expect and setting

$$i^2 = j^2 = k^2 = -1 \qquad ij = k \qquad jk = i \qquad ki = j.$$

It turns out that one can get a Galois extension $M/\mathbb{Q}$ with $\mathrm{Gal}(M/\mathbb{Q}) \cong Q_8$ by setting

$$M = \mathbb{Q}\left[\sqrt{(\sqrt{2}+2)(\sqrt{3}+3)}\right] = \mathbb{Q}[\alpha].$$

(a) M certainly contains the field $L = \mathbb{Q}[(\sqrt{2}+2)(\sqrt{3}+3)] \subseteq \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Why must L equal $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$?

Problem 4 - Continued. (b) We can get an isomorphism $Q_8 \cong \mathrm{Gal}(M/\mathbb{Q})$ by mapping i, j to automorphisms I, J determined by

$$I(\sqrt{2}) = -\sqrt{2} \qquad I(\sqrt{3}) = \sqrt{3} \qquad I(\alpha) = (\sqrt{2}-1)\alpha,$$

$$J(\sqrt{2}) = \sqrt{2} \qquad J(\sqrt{3}) = -\sqrt{3} \qquad J(\alpha) = \frac{3-\sqrt{3}}{\sqrt{6}}\alpha.$$

Compute what the automorphisms I^2 and IJ do on the elements $\sqrt{2}$, $\sqrt{3}$, and α.

(c) Given $I, J \in \mathrm{Gal}(M/\mathbb{Q})$ as defined above, what are the fixed fields of $\langle I \rangle$ and $\langle J \rangle$? What about the fixed fields of $\langle -1 \rangle$ and $\langle K \rangle$ for $-1 = I^2$ and $K = IJ$? (Make sure to justify both why your field is fixed by the subgroup, and why nothing larger than it is).

Problem 5. (a) What is the degree of the cyclotomic extension of 12-th roots of unity, $\mathbb{Q}(\zeta_{12})/\mathbb{Q}$? What are the possible images of ζ_{12} under automorphisms in $\mathrm{Gal}(\mathbb{Q}(\zeta_{12})/\mathbb{Q})$?

(b) Write down the minimal polynomial in $\mathbb{Q}[x]$ for $\zeta_{12} + \zeta_{12}^{-1}$ over $\mathbb{Q}$. Then write down the minimal polynomial in $\mathbb{Q}[x]$ for $\cos(\pi/6)$.

Problem 6. (a) Suppose that $f(x) \in \mathbb{Z}[x]$ is a monic irreducible polynomial with α a root, and that $g(x) \in \mathbb{Z}[x]$ is monic and has α^p as a root for a prime p. Show that $f(x)$ divides $g(x^p)$.

(b) Continuing from part (a), show that after reducing mod p, the polynomials $\overline{f}(x)$ and $\overline{g}(x)$ in $\mathbb{F}_p[x]$ have a common factor.

(c) Continuing from parts (a) and (b), show that the product $\overline{f}(x)\overline{g}(x)$ cannot divide a separable polynomial in $\mathbb{F}_p[x]$.