MA 553 Qualifying Exam *January 2009* Yu

- All notations are standard. Ask if there is anything you are not sure of.
- Each of Problems 4, 5, 7 is worth 10 points. Each part of the remaining problems is worth 5 points.
- You can always do a latter part by assuming the results in the previous parts—you will certainly need them for some of the problems—even if you have not solved the previous parts.
- Label your answers clearly.

1. Let $\mathbb{F}_q$ be a finite field with q elements.

(a) Show that $q = p^n$ for some prime number p and some integer $n \geq 1$.

(b) Show that the multiplicative group $\mathbb{F}_q^\times$ of $\mathbb{F}_q$, is cyclic of order $q-1$.

(c) Assume that q is odd. Let $a \in \mathbb{F}_q^\times$. Show that $x^2 = a$ has a solution with $x \in \mathbb{F}_q$ if and only if $a^{(q-1)/2} = 1$.

2. Let $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ be the quaternion group. We recall that it is a group of order 8, the elements $\pm i, \pm j, \pm k$ are of order 4, and the center of Q is the subgroup $\{\pm 1\}$ of order 2. Now assume that $L/\mathbb{Q}$ is a Galois extension with Galois group Q.

(a) How many subfields E of L are there such that $[E:\mathbb{Q}] = 2$? How many of them are normal over $\mathbb{Q}$?

(b) How many subfields E of L are there such that $[E:\mathbb{Q}] = 4$? How many of them are normal over $\mathbb{Q}$?

(c) Show that L is not the splitting field of any degree 4 polynomial over $\mathbb{Q}$.

(d) We know that L, being normal over $\mathbb{Q}$, is surely the splitting field of certain polynomial f over $\mathbb{Q}$. Determine the minimal degree of such an f.

3. Let $f(X) = X^3 + 2X^2 + 3X + 4$.

(a) Show that f is irreducible in $\mathbb{Q}[X]$.

(b) Let α be a (complex) root of $f(X)$ and put $E = \mathbb{Q}(\alpha)$. Find a formula for $N_{E/\mathbb{Q}}(\alpha + c)$ for any $c \in \mathbb{Q}$.

4. The discriminant of $X^3 + aX^2 + bX + c$ is $D = a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2$. Show that D, as an element in the polynomial ring $\mathbb{Q}[a,b,c]$, where a, b, c are indeterminates, is irreducible (you probably won't use how this polynomial D comes about in the proof).

5. Let $R = \mathbb{C}[X,Y]/I$, where X, Y are indeterminates, and I is the ideal generated by $X^3 - X - Y^2$. Therefore, if we denote the images of X and Y in R by x and y, respectively, then R is generated by x and y with the relation $x^3 - x = y^2$. Show that R is not a UFD (unique factorization domain).

6. Let $f: G \to H$ be a homomomorphism between two groups. Let $G^\#$ and $H^\#$ denote the set of conjugacy classes in G and H, respectively.

(a) Show that f induces a map $f^\#: G^\# \to H^\#$.

(b) Show that if $f^\#$ is injective, so is f.

(c) Show that if $f^\#$ is surjective, and if H is finite, then f is surjective (*Hint.* You can use the following fact freely: if H_0 is a proper subgroup of a finite group H, then $H \neq \bigcup_{x \in H} x H_0 x^{-1}$).

7. Let p be a prime number. Let K be a field of characteristic 0 such that K contains $\mu_p = \{x \in \bar{K} : x^p = 1\}$ (where $\bar{K}$ is an algebraic closure of K). Let $a, b \in K^\times$ and assume that the extension $L = K(a^{1/p}, b^{1/p})$ has degree p^2 over K. Show that the subfields lying in between K and L, are exactly K, L, $K(b^{1/p})$, and $K((ab^i)^{1/p})$, $i = 0, \ldots, p-1$.

8. Let μ_n be the group of complex n^{th} roots of 1, and put $E_n = \mathbb{Q}(\mu_n)$. Let $f = X^n - 1 \in \mathbb{Q}[X]$ and denote by (f) the ideal of $\mathbb{Q}[X]$ generated by f. Recall that $f(X) = \prod_{d|n} \Phi_d(X)$, where Φ_d is the d^{th} cyclotomic polynomial, which is irreducible by a theorem of Gauss.

(a) Show that E_n is isomorphic to $\mathbb{Q}[X]/(\Phi_n)$ as fields.

(b) Show that

$$\mathbb{Q}[X]/(f) \simeq \prod_{d|n} E_d.$$

That is, $\mathbb{Q}[X]/(f)$ is isomorphic to the direct product of E_d, for $d \mid n$, as rings.