QUALIFYING EXAMINATION
JANUARY 2005
MATH 553 - Prof. Yu

1. [15 points] Let $D_4 = \big\langle (1234), (12)(34) \big\rangle \subset S_4$ be the Dihedral group of order 8.

(a) Show that D_4 has exactly three subgroups H_1, H_2, H_3 of order 4.
(b) Show that exactly one of H_1, H_2, H_3 is cyclic.
(c) Show that $K = H_1 \cap H_2 \cap H_3$ is the commutator subgroup of D_4.

2. [20 points] Let s, t be indeterminates over $\mathbb{Q}$. Consider $F = \mathbb{Q}(s,t)$ and the polynomial $f = x^4 + sx^2 + t \in F[x]$. It is easy to verify

$$\begin{aligned} f(x) &= \left(x^2 - \frac{-s + \sqrt{s^2 - 4t}}{2}\right)\left(x^2 - \frac{-s - \sqrt{s^2 - 4t}}{2}\right) \\ &= \left(x^2 + \sqrt{2\sqrt{t} - s}\,x + \sqrt{t}\right)\left(x^2 - \sqrt{2\sqrt{t} - s}\,x + \sqrt{t}\right) \end{aligned}$$

Let E be the splitting field of f over F.

(a) Show that

$$\mathrm{Gal}(E/F(\sqrt{t})) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathrm{Gal}(E/F(\sqrt{s^2 - 4t})).$$

(b) Show that $\mathrm{Gal}(E/F) \simeq D_4$, the Dihedral group of order 8.
(c) Let K be the commutator subgroup of $\mathrm{Gal}(E/F) \simeq D_4$. Determine E^K.
(d) Let H be the unique subgroup of $\mathrm{Gal}(E/F)$ such that H is cyclic of order 4. Determine E^H.

3. [15 points] Let $q = p^m > 0$ be a prime power. Let $F = \mathbb{F}_q$ be a finite field of order q. An element $f(x) \in F[x]$ is called *monic* if its leading coefficient is 1, *square-free* if f is not divisible by g^2 for any non-zero $g \in F[x]$ of positive degree. For $n \geq 1$, let

$$\begin{aligned} P_n &= \{f \in F[x] : f \text{ is monic, irreducible, of degree } n\}, \\ Q_n &= \big\{f \in F[x] : f \text{ is monic, square-free, of degree } n\big\}. \end{aligned}$$

(a) Show that $\#P_2 = (q^2 - q)/2$, $\#Q_2 = q^2 - q$, here $\#X$ denotes the cardinality of the set X.
(b) Show that $\#Q_3 = q^3 - q$.
(c) Show that $\#Q_4 = q^4 - q$.

4. [15 points] Let F be a field of characteristic $p \geq 0$ and $f \in F[x]$ be a separable polynomial of degree n. Let $\alpha_1, \ldots, \alpha_n$ be the distinct roots of f (in a suitable extension field). Put

$$(*) \qquad a = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \alpha^0_{\sigma(1)} \alpha^1_{\sigma(2)} \cdots \alpha^{n-1}_{\sigma(n)} = \prod_{i<j} (\alpha_i - \alpha_j),$$

so that a^2 is the discriminant of f (you can take for granted that (*) is an equality). Let G be the Galois group of f, which is naturally a subgroup of S_n.

(a) Assume $p \neq 2$. Show that $G \subset A_n$ if and only if $a \in F$.

(b) Assume $p = 2$. Show that $a \in F$.

(c) Assume $p = 2$. Put $b = \sum_{\sigma \in A_n} \alpha^0_{\sigma(1)} \alpha^1_{\sigma(2)} \cdots \alpha^{n-1}_{\sigma(n)}$. Show that $G \subset A_n$ if and only if $b \in F$.

5. [10 points] Let F be a field. Let $F[x]$ be the polynomial ring over F and $F(x)$ the field of fractions of $F[x]$. Let R be the subring of $F(x)$ generated by $F[x]$ and x^{-1}. Show that R is a principal ideal domain.

6. [10 points] Let $n \geq 1$ be an integer, F a field. Show that

$$x^n + y^n + z^n$$

is irreducible in $F[x, y, z]$ if and only if $n \in F^\times$.

7. [10 points] Let E/F be a simple extension of fields of degree n.

(a) Regard E as a vector space over F. For $\alpha \in E$, let $f_\alpha : E \to E$ be the F-linear transformation defined by $f_\alpha(\beta) = \alpha\beta$. Show that $\alpha \mapsto f_\alpha$ is a ring homomorphism φ from E to the ring R of F-linear transformations from E to itself.

(b) Notice that $R \simeq M_n(F)$, the ring of $n \times n$ matrices over F. Show that there is no ring homomorphism $E \to M_{n-1}(F)$.

8. [15 points] Let G be a finite group of order $2^e n$, where n is odd. Assume that the Sylow 2-subgroups of G are cyclic.

(a) Show that if H is a subgroup of G, then the Sylow 2-subgroups of H are cyclic.

(b) Let $u \in G$ be such that $\langle u \rangle$ is a Sylow 2-subgroup. Let $R : G \to S_G$ be such that $R(g)$ is the permutation sending x to gx. Show that $R(u)$ is an odd permutation.

(c) Show that G contains a subgroup of index 2^i, for $i = 1, 2, \ldots, e$.