MATH 553 QUALIFYING EXAMINATION, JANUARY 2013

READ THIS $\Longrightarrow$: PLEASE BEGIN EACH QUESTION **(I–V)** ON A NEW SHEET OF PAPER.

IN ANSWERING ANY PART OF A QUESTION, YOU MAY ASSUME THE RESULTS IN PREVIOUS PARTS, EVEN IF YOU HAVEN'T DONE THEM.

[**Bold numbers**] INDICATE POINTS (**60** TOTAL).

I. This problem indicates that to classify groups G of order pqr, where $p > q > r$ are prime, one can start by showing that G is isomorphic to a semidirect product $P \rtimes_\theta K$ where P has order p and K has order qr.

By counting elements of order p or q, one sees that in such a G, *either there is a normal Sylow p-subgroup or there is a normal Sylow q-subgroup.* (You may assume this.) Prove:

(a) [**5**] G has a subgroup H of order pq; and H is *normal* in G.

(b) [**4**] Every subgroup of G of order p or q is contained in H.

(c) [**5**] G has exactly one subgroup P of order p.

(d) [**6**] G has a subgroup K of order qr.

Hint. When G has more than one subgroup of order q, consider the normalizer of any one of them.

II. Let R be a ring such that $x^2 = x$ for all $x \in R$. (Such rings are called *Boolean.*) Prove:

(a) [**1**] In R, 2=0.

(b) [**2**] R is commutative. (Hint: expand $(x+y)(x+y)$.)

(c) [**3**] For an ideal $p \neq R$, the following conditions are equivalent:
(i) p is prime.
(ii) For every $x \in R$, either $x \in p$ or $1 - x \in p$.
(iii) $R/p \cong \mathbb{F}_2$, the field with two elements.

(d) [**4**] Let S be the set of prime ideals in R. Then R is isomorphic to a subring of the ring of all maps of sets $S \to \mathbb{F}_2$—where the sum and product of two maps f, g are given by

$$(f+g)(p) = f(p) + g(p), \qquad (fg)(p) = f(p)g(p).$$

Hint: For $x \in R$, consider the map x^* given by $x^*(p) = (x + p) \in R/p$.

III. Let ω be the complex number $\big(1 + i\sqrt{11}\,\big)/2$.

(a) [**2**] Show that $\mathbb{Z}[\omega]$ is norm-euclidean.

(b) [**2**] Prove that 2 is prime in $\mathbb{Z}[\omega]$, but not in $\mathbb{Z}[2\omega]$.

(c) [**3**] Let $p \neq 11$ be an odd positive prime in $\mathbb{Z}$, let ζ be a primitive 11-th root of unity in some extension of the finite field $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

It is known (and you may assume) that the "Gauss sum" $\xi := \sum_{i=1}^{5} \zeta^{i^2} = \zeta + \zeta^4 + \zeta^9 + \zeta^5 + \zeta^3$ satisfies $(2\xi + 1)^2 = -11$. Show that

$$-11 \text{ is a square in } \mathbb{F}_p \iff \xi^p = \xi \iff p \text{ is a square in } \mathbb{F}_{11}.$$

(d) [**3**] Show: p (as in (c)) $= x^2 + xy + 3y^2$ for some $x, y \in \mathbb{Z} \iff p \equiv 1,\ 3,\ 4,\ 5, \text{ or } 9 \pmod{11}$.

IV. (a) **[2]** Let G be a cyclic group of order g, and let $n > 0$ be a divisor of g. Prove that the set

$$\{\, x \in G \mid x^n = e \,\} \qquad (e = \text{identity})$$

is the unique subgroup of order n in G.

(b) **[4]** Let $F = \mathbb{F}_q$ be a finite field of cardinality $|F| = q$, and let n be a positive integer relatively prime to q. Prove that a field $K \supset F$ contains a splitting field L (over F) of the polynomial $X^n - 1$ if and only if n divides $|K| - 1$; and deduce that the degree $[L : F]$ is the order of q in the multiplicative group of units of $\mathbb{Z}/(n)$.

(c) **[4]** Factor the polynomial $X^{12} - 1 \in \mathbb{F}_5[X]$ into irreducibles.

V. Let k be a commutative field, and let $k(X)$ be the field of fractions of the polynomial ring $k[X]$. Let f and g be the unique automorphisms of $k(X)$ fixing k and such that

$$f(X) = 1/X, \qquad g(X) = 1 - X.$$

In the group of all automorphisms of $k(X)$, let G be the subgroup generated by f and g.

(a) **[3]** Write down explicitly all the members of G. (f and g are already given above; specify the other members similarly.)

(b) **[3]** Show that the fixed field of G is $k(Y)$, where

$$Y = (X^2 - X + 1)^3/(X^2 - X)^2.$$

(c) **[4]** Show: If $k(Y) \subsetneqq L \subsetneqq k(X)$ with $L/k(Y)$ a normal field extension, then $L = k(Z)$ where

$$Z = X + \left(1 - \frac{1}{X}\right) + \frac{1}{1 - X}\ .$$