QUALIFYING EXAMINATION
AUGUST 2003
MATH 553 - Prof. Lipman

Begin each question (I-IV) 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. Let G be a group of order pqr, where $p > q > r$ are prime. Prove:

(a) [**6**] If G has no normal subgroup of order p, then G has exactly $pqr - qr$ elements of order p.

(b) [**6**] If G has no normal subgroup of order q, then G has more than q^2 elements of order q.

(c) [**6**] G is solvable.

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) $R/pR \cong \mathbb{F}_2$, 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 $S \to \mathbb{F}_2$ [with sum and product of two maps f, g 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 $x^*(p) = (x + pR) \in R/pR$. Note that $x^* \equiv 0$ implies that $1 - x$ is a unit. (You may assume the result that every non-unit ideal is contained in a maximal ideal.)

III. (a) [**3**] Prove that the ring $R = \mathbb{Z}[\sqrt{-2}\,]$ is Euclidean.

(b) [**3**] Show that $R/(3 + 2\sqrt{-2}\,)$ is a field. What is the characteristic of this field?

(c) [**4**] Show that the polynomial $X^4 + 3$ is irreducible over the field $\mathbb{F}_{17}$ of 17 elements; and deduce that $f(X) = X^4 - 170X^3 + 9 + 4\sqrt{-2} \in R[X]$ is irreducible.

(d) [**2**] Is the polynomial $Y^4 - f(X) \in R[X, Y]$ irreducible? (Why?)

IV. Let K be a field of characteristic $p \geq 0$, and n a positive integer not divisible by p. Let $0 \neq a \in K$, let L be a splitting field over K of the polynomial $X^n - a$, and let $\alpha \in L$ be a root of this polynomial.

(a) [**3**] Prove that L contains an element ζ which has exactly n distinct powers.

(b) [**5**] Prove that the galois group $\mathcal{G}\big(L/K(\zeta)\big)$ is cyclic of order n/e, where e is the largest divisor of n such that a is an e-th power in $K(\zeta)$.

Hint: If f divides n then a is an f-th power in $K(\zeta) \iff \alpha^{n/f}$ is $\mathcal{G}$-invariant.

(c) [**4**] Calculate the degree $[K(\alpha) : K(\alpha) \cap K(\zeta)]$.

(d) **[6]** Set $\beta := \alpha^{n/e} \in K(\zeta)$. Prove that for each divisor d of n/e there is a unique field F isomorphic to $K(\zeta)[X]/(X^d - \beta)$ and such that $K(\zeta) \subset F \subset L$; and that there are no other fields between $K(\zeta)$ and L.

(e) **[2]** Prove that the monic irreducible factors of $X^n - a$ in $K(\zeta)[X]$ are the e polynomials

$$X^{n/e} - (\zeta^i \alpha)^{n/e}, \qquad 0 \le i < e.$$