553 Final exam, due 10AM, April 29, 2013

Write your name in the top left corner. Attempt all questions.

1. Let G be a group. If S is a simple group, S is said to *occur* in G if there exist two subgroups H and H' of G, with $H \lhd H'$, such that $H'/H \simeq S$. Let $\mathrm{In}(G)$ be the set of isomorphism classes of simple groups occurring in G.

   i. $\mathrm{In}(G) = \emptyset \Longrightarrow G = \{e\}$.

   ii. If H is a subgroup of G, show that $\mathrm{In}(H) \subset \mathrm{In}(G)$; if H is normal, show that $\mathrm{In}(G) = \mathrm{In}(H) \cup \mathrm{In}(G/H)$.

   iii. Let G_1, G_2 be two groups. Show that the following two properties are equivalent.

      a) $\mathrm{In}(G_1) \cap \mathrm{In}(G_2) = \emptyset$;

      b) Every subgroup of $G_1 \times G_2$ is of the form $H_1 \times H_2$, where H_1 is a subgroup of G_1, and H_2 a subgroup of G_2.

2. Let G be a finite group and p a prime number. An element $g \in G$ is called *p-unipotent* if its order is a power of p, and *p-regular* if its order is not divisible by p.

   i. Let $x \in G$. Show that there exists a unique ordered pair (u, r) of elements of G such that u is p-unipotent, and r is p-regular, and $s = ur = ru$. (Hint: First consider the case where G is the cyclic group generated by x.)

   ii. What "theorem" from linear algebra does (i) remind you of ?

   iii. Let P be a p-Sylow subgroup of G, C the centralizer of P, and E the set of p-regular elements of G. Show that $|E| = |E \cap C| \bmod p$.

   iv. Deduce that p does not divide $|E|$. (Hint: Use induction on the cardinality of G to reduce to the case where $C = G$; then use (i)).

3. Let G be a finite group with $|G| = p^k m$, where p is a prime but m not necessarily co-prime to p. Let S be the set of p^k-element subsets of G. Prove the following.

   i.
   $$\frac{|S|}{m} = \binom{p^k m - 1}{p^k - 1}.$$

ii. $\dfrac{|S|}{m} = 1 \bmod p$.

iii. Let G act on S be left translation. If $A \in S$, prove that the order of the isotropy subgroup G_A divides p^k.

iv. Let $S_0 = \{A \in S \,|\, |G_A| = p^k\}$. Show that $|S| = |S_0| \bmod pm$.

v. Prove that

$$S_0 \;=\; \{Hx |\; H \text{ subgroup of } G \text{ with } |H| = p^k \text{ and } x \in G\}.$$

vi. Conclude that the number of subgroups of G of order p^k is $1 \bmod p$.

4.

i. Let k be a field, and $k[x]$ a polynomial ring. Prove that $k[x]$ contains infinitely many distinct monic irreducible polynomials.

ii. If A is an integral domain which is not a field, prove that $A[x]$ is *not* a principal ideal domain.

iii. Let $f \in \mathbb{Z}[x]$ be a monic polynomial. If $f(a) = 0$ for some $a \in \mathbb{Q}$, prove that $a \in \mathbb{Z}$.

5. Let A be a ring with a unit element such that $x^3 = x$ for all $x \in A$. The goal is to prove that A is commutative.

i. Show that $6A = 0$ and that $2A$ and $3A$ are two-sided ideals such that $2A + 3A = A$ and $2A \cap 3A = 0$. Deduce that it can be assumed that either $2A = 0$ or $3A = 0$ (for the purpose of this problem).

ii. Prove that A is commutative.

6. Prove or disprove with a counter-example. Let E/F be a finite field extension. Then, there are only a finite number of subfields of E containing F.

7. Page 582, Problem 15.

8. Page 582, Problem 16.

9. Page 583, Problem 27.

10. Page 585, Problem 29.