Homework 7, due on Friday, October 23

Read carefully chapters 14,15, 16 in the textbook and the notes for the lectures on the course web page. **It is crucial that you read and attempt ALL the exercises at the end of each chapter as they form integral part of the book.**
Solve the following problems.

Problem 1. a) List all abelian groups of order 4225 (up to isomorphism).

b) Let m, n be positive integers and let $d = \gcd(m, n)$ and $l = \text{lcm}(m, n)$. Prove that $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_d \times \mathbb{Z}_l$. Hint: do this first when $d = 1$ (we basically did it in class), then use factorization into prime powers of m, n, d, l and rearrange. It may be helpful to work out the case when $m = 540$ and $n = 600$ first.

Problem 2. Call a group G an H-group if every subgroup of G is normal in G.

a) Show that any subgroup of an H-group is also an H-group.

b) Let G be an H-group and $f : G \longrightarrow K$ a surjective homomorphism. Prove that K is an H-group.

c) Let G and H be groups with no elements of infinite order (such groups are called **torsion**). Suppose that for any $a \in G$ and $b \in H$ the orders of a and b are relatively prime. Let T be a subgroup of $G \times H$. Prove that $T = A \times B$ for a subgroup A of G and a subgroup B of H. Prove that T is normal if and only if both A and B are normal in G, H respectively.

d) In part c) assume that both G and H are H-groups. Prove that $G \times H$ is an H-group.

Problem 3. a) Let G be a group and a, b elements in G such that the cyclic subgroups $< a >$ and $< b >$ are normal in G. Prove that if $< a >$ has infinite order then either $ba = ab$ or $ba = a^{-1}b$. Then prove that the latter case is not possible, i.e. a and b must commute.

b) Let G be an H-group which has an element of infinite order. Prove that G is abelian.

Let G be a nonabelian H-group. Thus by b) each element in G has finite order.

c) Suppose that $a, b \in G$ have odd order. Prove that ab also has odd order. Hint: prove that the subgroup $< a >< b >$ has odd order. Conclude that the set T of all elements of odd order in G is a subgroup.

d) Suppose that $a, b \in G$ have order which is a power of 2. Prove that the order of ab is also a power of 2. Conclude that the set D of all elements in G whose order is a power of 2 is a subgroup.

e) Prove that $G \cong D \times T$.

f) Conversely, suppose that D is an H-group in which the order of every element is a power of 2 and T is an H-group in which every element has odd order. Show that $D \times T$ is an H-group (use problem 2d)).

Remark. One can show that any H-group T in which every element has odd order is abelian. A group D in which the order of every element in a power of 2 is an H-group if

and only if either D is abelian or $D \cong Q_8 \times A$ where Q_8 is the quaternion group and A is a group in which every non-identity element has order 2.

Problem 4. Let G be a finite group and p a prime number such that $p||G|$. Consider the set S of all $p-$tuples $(a_1, ..., a_p)$ of elements from G such that $a_1a_2...a_p = e$, i.e.

$$S = \{(a_1, ..., a_p) : a_i \in G \text{ for all } i, \text{ and } a_1...a_p = e\}$$

Let C be a cyclic group of order p and f a generator for C. We define an action of C on S as follows: if $s \in C$ then $s = f^i$ for a unique $0 \leq i < p$ and we set $s * (a_1, ..., a_p) = (a_{i+1}, a_{i+2}, ...a_p, a_1, a_2, ..., a_i)$.

a) Check that this is indeed an action of C on S. Hint: show that if in a group we have $a_1a_2 \dots a_n = e$ then $a_2 \dots a_na_1 = e$.

b) Show that the number of elements in S equals $|G|^{p-1}$ (note that any choice of $a_1, \dots, a_{p-1}$ uniquely determines a_p).

c) Show that an element in S has orbit consisting of only 1 element (i.e. is a fixed point for this action) if and only if it is of the form $(g, ..., g)$ for some $g \in G$ such that $g^p = e$.

d) Note that the cardinality of S is divisible by p and the size of each orbit is either 1 or p. Conclude that the number of orbits with 1 element is divisible by p.

d) Conclude that G has an element of order p.

The following problems are optional.

Problem 5. Let p be a prime number and let $P = \mathbb{Z}_{p^{m_1}} \times \mathbb{Z}_{p^{m_2}} \times \dots \times \mathbb{Z}_{p^{m_k}}$ for some $m_1 \geq m_2 \geq \dots \geq m_k \geq 1$.

a) Consider the subgroup $P_1 = \{a \in P : a^p = e\}$. Show that P_1 has p^k elements. Thus k is uniquely determined by P.

b) Consider the subgroup $P_2 = \{a \in P : a^{p^2} = e\}$. Show that P_2 has p^{2k-r} elements, where r is the number of indexes i such that $m_i = 1$. Conclude that r is uniquely determined by P.

c) Prove that $P/P_1 \cong \mathbb{Z}_{p^{m_1-1}} \times \mathbb{Z}_{p^{m_2-1}} \times \dots \times \mathbb{Z}_{p^{m_{k-r}-1}}$.

d) Use c) and induction to prove that the sequence $m_1, m_2, \dots, m_k$ is uniquely determined by P.