Math 322: Problem Set 8 (due 6/11/2014)

P1. Let G be a commutative group and let $k \in \mathbb{Z}$.
  (a) Show that the map $x \mapsto x^k$ is a group homomorphism $G \to G$.
  (b) Show that the subsets $G[k] = \left\{g \in G \mid g^k = e\right\}$ and $\left\{g^k \mid g \in G\right\}$ are subgroups.
  RMK For a general group G we let $G^k = \left\langle \left\{g^k \mid g \in G\right\} \right\rangle$ be the subgroup generated by the kth powers. You have shown that, for a commutative group, $G^k = \left\{g^k \mid g \in G\right\}$.

Cyclic groups and their automorphisms

1. (Structure of cyclic groups)
  (a) Let G be a group, $g \in G$ an element of order n, and let $a \in \mathbb{Z}$ Show that g^a has order $\frac{n}{\gcd(n,a)}$.
  (b) Show that C_n has $\phi(n)$ generators, where $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$ is the Euler totient function.
  (c) Let $A = \mathbb{Z}/n\mathbb{Z}$. Show that if $d|n$ then $A[d] = \{a \in A \mid d \cdot a = [0]\}$ (see problem P1) is the subgroup generated by the residue class of $\frac{n}{d}$.
  (d) Show that C_n has a unique subgroup of order d for each $d|n$.

2. We show "If G has order n, and for every $d|n$ there is at most one subgroup of order d then G is cyclic". For this let G be a minimal counterexample.
  (a) Show that every proper subgroup of G is cyclic.
  (b) Show that, for each $d|n$, G has at most $\phi(d)$ elements of order exactly d (hint: let $g \in G$ have order d; what can you say about $\langle g \rangle$?)
  (c) Use the formula $\sum_{d|n} \phi(d) = n$ show that G is cyclic.

PRAC Let F be a field, and let $H \subset F^\times$ be a finite group.
  (a) Show that for each positive integer d, H has at most d elements of order dividing d (hint: express the statement "x has order dividing d" by a polynomial equation, and use the fact that a polynomial of order d over a field has at most d roots).
  (b) Show that H is cyclic.

Automorphisms of groups and semidirect products

3. Let H,N be groups, and let $\varphi \in \mathrm{Hom}(H, \mathrm{Aut}(N))$ be an action of H on N by automorphisms.
  DEF The (external) *semidirect product* of H and N *along* φ is the operation

$$(h_1,n_1) \cdot (h_2,n_2) = \left(h_1h_2, \left(\varphi(h_2^{-1})n_1\right) n_2\right)$$

  on the set $H \times N$. We denote this group $H \ltimes_\varphi N$.
  PRAC Verify that when φ is the trivial homomorphism ($\varphi(h) = \mathrm{id}$ for all $h \in H$), this is the ordinary direct product.
  (a) Show that the semidirect product is, indeed, a group.
  (b) Show that $f_H \colon H \to H \ltimes_\varphi N$ given by $f(h) = (h,e)$, $f_N \colon N \to H \ltimes_\varphi N$ given by $f(n) = (e,n)$ and $\pi \colon H \ltimes_\varphi N \to H$ given by $\pi(h,n) = h$ are group homomorphisms.
  (c) Show that $\tilde{H} = f_H(H)$ and $\tilde{N} = f_N(N)$ are subgroups with $\tilde{N}$ normal. Show that for $\tilde{h} = (h,e)$ and $\tilde{n} = (e,n)$ we have $\tilde{h}\tilde{n}\tilde{h}^{-1} = \widetilde{(\varphi(h))(n)}$.
  (d) Show that $H \ltimes_\varphi N$ is the internal semidirect product of its subroups $\tilde{H}$, $\tilde{N}$.

Supplementary problems

A. Let D_{2n} be the dihedral group, acting on the graph with vertices $\{1,2,\cdots,n\}$ and edges $\{\{1,2\},\{2,3\},\ldots,\{n,1\}\}$.

PRAC Let $c=(123\cdots n)\in D_{2n}$ be the "rotation" and let $r(i)=n+1-i$ be the "reflection". Show that $r,c\in D_{2n}$.

(a) Show that $C=\langle c\rangle\simeq C_n$ and that $R=\langle r\rangle\simeq C_2$. Show that R normalizes C.

(b) Show that $D_{2n}=R\ltimes C$, and in particular that every element of D_{2n} is either of the form c^j or rc^j.

(c) Give the multiplication rule in those coordinates. In particular, show that all the elements of the form rc^j are of order 2.

(d) Find all the conjugacy classes in D_{2n}.

Solving the following problem involves many parts of the course.

B. Let G be a group of order 8.

(a) Suppose G is commutative. Show that G is isomorphic to one of C_8, $C_4\times C_2$, $C_2\times C_2\times C_2$.

(b) Suppose G is non-commutative. Show that there is $a\in G$ of order 4 and let $H=\langle a\rangle$.

(c) Show that $a\notin Z(G)$ but $a^2\in Z(G)$.

(d) Suppose there is $b\in G-H$ of order 2. Show that $G\simeq D_8$ (hint: $bab^{-1}\in\left\{a,a^3\right\}$ but can't be a).

(e) Let $b\in G-H$ have order 4. Show that $bab^{-1}=a^3$and that $a^2=b^2=(ab)^2$.

(f) Setting $c=ab$, $-1=a^2$ and $-g=(-1)g$ show that $G=\{\pm1,\pm a,\pm b,\pm c\}$with the multiplication rule $ab=c$, $ba=-c$, $bc=a$, $cb=-a$, $ca=b$, $ac=-b$.

(g) Show that the set in (f) with the indicated operation is indeed a group.

DEF The group of (f),(g) is called the *quaternions* and indicated by Q.

Supplement: *p*-Sylow subgroups

C. Let G be a group (especially infinite).

DEF Let X be a set. A *chain* $\mathcal{C}\subset P(X)$ is a set of subsets of X such that if $A,B\in\mathcal{C}$ then either $A\subset B$ or $B\subset A$.

(a) Show that if $\mathcal{C}$ is a chain then for every finite subset $\{A_i\}_{i=1}^n\subset\mathcal{C}$ there is $B\in\mathcal{C}$ such that $A_i\subset B$ for all i.

(b) Suppose $\mathcal{C}$ is a non-empty chain of subgroups of a group G. Show that the union $\bigcup\mathcal{C}$ is a subgroup of G containing all $A\in cC$.

(c) Suppose $\mathcal{C}$ is a chain of p-subgroups of G. Show that $\bigcup\mathcal{C}$ is a p-group as well.

(*d) Use Zorn's Lemma to show that every group has maximal p-subgroups (p-subgroups which are not properly contained in other p-subgroups), in fact that every p-subgroup is contained in a maximal one.

RMK When G is infinite, it does not follow that these maximal subgroups are all conjugate.