Lior Silberman's Math 322: Problem Set 8 (due 9/11/2017)

On group actions and homomorphisms

1. Let the group G act on the set X.
   DEF The *kernel* of the action is the normal subgroup $K = \{g \in G \mid \forall x \in X : g \cdot x = x\}$.
   PRAC K is the kernel of the associated homomorphism $G \to S_X$, hence $K \lhd G$ indeed.
   (a) Construct an action of G/K on X "induced" from the action of G.
   DEF An action is called *faithful* its the kernel is trivial.
   (b) Show that the action of G/K on X is faithful.
   SUPP Show that this realizes G/K as a subgroup of S_X.
   (c) Suppose G acts non-trivially on a set of size n. Show that G has a proper normal subgroup of index at most $n!$.
   (*d) Show that an infinite simple group has no proper subgroups of finite index.

*2. Let G be a group of finite order n, and let p be the smallest prime divisor of n. Let $M < G$ be a subgroup of index p. Show that M is normal.
   RMK In particular, this applies when G is a finite p-group.

Automorphisms of groups and semidirect products

Recall that $\mathrm{Aut}(H)$ is the group of isomorphisms $H \to H$.

*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. We write φ_h rather than $\varphi(h)$ for the automorphism given by $h \in H$, so result of h acting on n (the result of applying the automorphism $\varphi(h)$ to n) will be written $\varphi_h(n)$. That φ is a homomorphism is the statement that $\varphi_h \circ \varphi_{h'} = \varphi_{hh'}$.
   DEF The (external) *semidirect product* of H and N *along* φ is the operation
   $$(h_1, n_1) \cdot (h_2, n_2) = \left(h_1 h_2, \left(\varphi_{h_2^{-1}}(n_1)\right) n_2\right)$$
   on the <u>set</u> $H \times N$. 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 $\tilde{H}$, $\tilde{N}$.

4. (Concrete 3(b),(c),(d)) Let $H=\mathbb{R}^\times$ act on $N=\mathbb{R}$ by multiplication (so $\varphi_h(n)=hn$). Show $H\ltimes_\varphi N$ is isomorphic to the subgroup $P=\left\{\begin{pmatrix} h & n \\ & 1\end{pmatrix} \mid h\in\mathbb{R}^\times, n\in\mathbb{R}\right\}$ of $\mathrm{GL}_2(\mathbb{R})$.

   SUPP Do the same with $H=(\mathbb{Z}/n\mathbb{Z})^\times$, $N=\mathbb{Z}/n\mathbb{Z}$. Now P is a finite group.

   SUPP Same with $H=\mathrm{GL}_d(\mathbb{R})$, $N=\mathbb{R}^d$, $P=\left\{\begin{pmatrix} h & \underline{n} \\ & 1\end{pmatrix} \mid h\in\mathrm{GL}_d(\mathbb{R}), \underline{n}\in\mathbb{R}^d\right\} < \mathrm{GL}_{d+1}(\mathbb{R})$.

5. (Cyclic groups)
   (a) Let A be a group. Show that mapping $f\in\mathrm{Hom}(C_n,A)$ to $f([1]_n)$ gives a bijection between $\mathrm{Hom}(C_n,A)$ and the set of $a\in A$ of order dividing n.
   (b) Write f_a for the homomorphism such that $f([1])=a$. When $A=C_n=(\mathbb{Z}/n\mathbb{Z},+)$ show that $f_a\circ f_b=f_{ab}$ (ab is multiplication mod n) and hence that $\mathrm{Aut}(C_n)\simeq(\mathbb{Z}/n\mathbb{Z})^\times$.

   RMK You've just done a fancy version of problem 4 of PS1

Extra Credit

6. The two parts complete problem 3. For these let $\varphi\in\mathrm{Hom}(H,\mathrm{Aut}(N))$.
   (a) For $\alpha\in\mathrm{Aut}(H)$ define $\psi\colon H\to\mathrm{Aut}(N)$ by $\psi=\varphi\circ\alpha$ (that is $\psi_h=\varphi_{\alpha(h)}$). Show that $F(h,n)=\left(\alpha^{-1}(h),n\right)$ gives an isomorphism $F\colon H\ltimes_\varphi N\to H\ltimes_\psi N$.
   (b) For $\beta\in\mathrm{Aut}(N)$ define $\psi\colon H\to\mathrm{Aut}(N)$ by $\psi_h=\beta\circ\varphi_h\circ\beta^{-1}$ (this is conjugation in $\mathrm{Aut}(N)$!). Show that $H\ltimes_\varphi N\simeq H\ltimes_\psi N$.
   (c) Let $a,b\in\mathrm{Aut}(N)$ generate the same cyclic subgroup, and let $f_a,f_b\in\mathrm{Hom}(C_n,\mathrm{Aut}(N))$ be the maps from 5(b). Show that $C_n\ltimes_{f_a}N\simeq C_n\ltimes_{f_b}N$

   RMK From (b),(c) we conclude and conclude that semidirect products $C_n\ltimes N$ are determined by *conjugacy classes of subgroups* of $\mathrm{Aut}(N)$ which are cyclic of order dividing n.

Supplementary problems

A. We show that $(\mathbb{Z}/p\mathbb{Z})^\times \simeq C_{p-1}$ so that $\mathrm{Aut}(C_p) \simeq C_{p-1}$.
   (a) Let F be a field. Show that $F^\times$ has at most d elements of order dividing d (hint: a polynomial of degree d over a field has at most d roots).
   (b) Let $H < F^\times$ be a finite group. Show that H is cyclic.
   (c) Show that $\mathrm{Aut}(C_p) \simeq C_{p-1}$.

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 $G = \{\pm 1, \pm a, \pm b, \pm c\}$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.

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-subgrounps), 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.