Math 322: Problem Set 7 (due 30/10/2014)

Practice problems

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, $G^k = \left\{g^k \mid g \in G\right\}$.

P2. Let G commutative group where every element has order dividing p.

(a) Endow G with the structure of a vector space over $\mathbb{F}_p$.

(b) Show that $\dim_{\mathbb{F}_p} G = k$ iff $\#G = p^k$ iff $G \simeq (C_p)^k$.

(c) Show that for any $X \subset G$, we have$\langle X \rangle = \mathrm{Span}_{\mathbb{F}_p} X$.

P3. For a field F let $H = \left\{ \begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix} \mid x, y, z \in F \right\}$ is called the *Heisenberg group* over F.

(a) Show that H is a subgroup of $\mathrm{GL}_3(F)$ (you also need to show containment, that is that each element is an invertible matrix).

(b) Show that $Z(H) = \left\{ \begin{pmatrix} 1 & 0 & z \\ & 1 & 0 \\ & & 1 \end{pmatrix} \mid z \in F \right\} \simeq F^+$.

(c) Show that $H/Z(H) \simeq F^+ \times F^+$ via the map $\begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix} \mapsto (x, y)$.

(d) Show that H is non-commutative, hence is not isomorphic to the direct product $F^2 \times F$.

(e) Suppose $F = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Then $\#H = p^3$ so that H is a p-group. Show that every element of $H(\mathbb{F}_p)$ has order p.

General theory

Fix a group G.

1. (Correspondence Theorem) Let $f \in \mathrm{Hom}(G, H)$, and let $K = \mathrm{Ker}(f)$.

(a) Show that the map $M \mapsto f(M)$ gives a bijection between the set of subgroups of G containing K and the set of subgroups of $\mathrm{Im}(f) = f(G)$.

(b) Show that the bijection respects inclusions, indices and normality (if $K < M_1, M_2 < G$ then $M_1 < M_2$ iff $f(M_1) < f(M_2)$, in which case $[M_2 : M_1] = [f(M_2) : f(M_1)]$, and $M_1 \lhd M_2$ iff $f(M_1) \lhd f(M_2)$).

2. Let $X, Y \subset G$ and suppose that $N = \langle X \rangle$ is normal in G. Let $q \colon G \to G/N$ be the quotient map. Show that $G = \langle X \cup Y \rangle$ iff $G/N = \langle q(Y) \rangle$.

3. 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 $K \triangleleft G$ 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.

**4. 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.

p-groups

5. Recall the group $\mathbb{Z}\left[\frac{1}{p}\right] = \left\{\frac{a}{p^k} \in \mathbb{Q} \mid a \in \mathbb{Z}, k \geq 0\right\} < \mathbb{Q}^+$, and note that $\mathbb{Z} \triangleleft \mathbb{Z}\left[\frac{1}{p}\right]$ (why?).
(a) Show that $G = \mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z}$ is a p-group.
(b) Show that for every $x \in G$ there is $y \in G$ with $y^p = x$ (warning: what does y^p mean?)

*6. If $|G| = p^n$, show for each $0 \leq k \leq n$ that G contains a normal subgroup of order p^k.

7. Let G be a finite p-group, and let $H \triangleleft G$. Show that if H is non-trivial then so is $H \cap Z(G)$.

Supplement: Generation of finite p-groups

A. Let G be a finite commutative p-group.
(a) Show that G^p is a proper subgroup (problem P1 is relevant here).
(b) Show that G/G^p is a non-trivial commutative group where every element has order p.
— Let $X \subset G$ be such that its image under the quotient map generates G/G^p.
(c) For $k \geq 0$ let $g_k \in G^{p^k}$ ($G^1 = G$). Show that there is $w \in \langle X \rangle$ and $g_{k+1} \in G^{p^{k+1}}$ such that $g_k = w^{p^k} g_{k+1}$.
(d) Suppose that $\#G = p^n$. Show that $G^{p^n} < \langle X \rangle$, and then by backward induction eventually show that $G = G^1 < \langle X \rangle$.
RMK You have proved: X generates G iff $q(X)$ generates G/G^p. In particular, the minimal number of generators is exactly $\dim_{\mathbb{F}_p} G/G^p = \log_p [G : G^p]$.

RMK In fact, for any p-group, G, X generates G iff its image generates $G/G'G^p$ where G' is the derived (commutator) subgroup.