Math 322: Problem Set 7 (due 5/11/2015)

Practice problems

P1. 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 $\langle X \rangle = \mathrm{Span}_{\mathbb{F}_p} X$.

P2. The group $H = \left\{ \begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix} \mid x, y, z \in F \right\}$ is called the *Heisenberg group* over the field 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 $F = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ with p odd. 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*. Suppose G is finite and let H be a proper subgroup. Show that the conjugates of H do not cover G (that is, there is some $g \in G$ which is not conjugate to an element of H).

2. (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 $f(M_1) \lhd f(M_2)$).

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

p-groups

4. 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 $\mathbb{Z} \lhd \mathbb{Z}\left[\frac{1}{p}\right]$ (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?)

SUPP Show that every proper subgroup of G is finite and cyclic. Conversely, for every k there is a unique subgroup isomorphic to p^k.

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

Bonus problem

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

Supplement: Group actions

A. Fix an action $\cdot$ of the group G on the set X.
   (a) Let $Y \subset X$ be *G-invariant* in that $gY = Y$. Show that the *restriction* $\cdot \restriction_{G \times Y}$ defines an action of G on Y.
   (b) Let $H < G$. Show that the *restriction* $\cdot \restriction_{H \times X}$ defines an action of H on X.
   (c) Show that every G-orbit in X is a union of H-orbits.
   (d) Show that every G-orbit is the union of at most $[G : H]$ H-orbits.

B. Let the finite group G act on the finite set X.
   DEF For $g \in G$ its *set of fixed points* is $\mathrm{Fix}(g) = \{x \in X \mid g \cdot x = x\}$. The *stabilizer* of $x \in X$ is $\mathrm{Stab}_G(x) = \{g \in G \mid g \cdot x = x\}$.
   (a) Enumerating the elements of the set $\{(g,x) \in G \times X \mid g \cdot x = x\}$ in two different ways, show that
$$\sum_{g \in G} \#\mathrm{Fix}(g) = \sum_{x \in X} \#\mathrm{Stab}_G(x)\,.$$
   (b) Using the conjugacy of point stabilizers in an orbit, deduce that
$$\sum_{g \in G} \#\mathrm{Fix}(g) = \sum_{\mathcal{O} \in G \backslash X} \#G$$
   and hence the *Lemma that is not Burnside's:* the number of orbits is exactly the average number of fixed points,
$$\#G \backslash X = \frac{1}{\#G} \sum_{g \in G} \#\mathrm{Fix}(g)\,.$$
   (c) Example: suppose we'd like to colour each vertex of a cube by one of four different colours, with two colourings considered equivalent if they are obtained from each other by a rotation of the cube. How many colourings are there, up to equivalence?

(hint for 1: count elements)
(hint for 5: adapt a proof from class)

Supplement: Generation of finite commutative 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.