Math 322: Problem Set 7 (due 2/11/2015)

Practice problem

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$\langle X\rangle = \mathrm{Span}_{\mathbb{F}_p} X$.
  (d) Show that any generating set of $\mathbb{C}_2^k$ consists of at least $k = \log_2\left(\#C_2^k\right)$ elements.

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. Let $\mathbb{Z}\left[\frac{1}{p}\right] = \left\{\frac{a}{p^k} \in \mathbb{Q} \mid a \in \mathbb{Z}, k \geq 0\right\} < (\mathbb{Q},+)$, and note that $\mathbb{Z} \lhd \mathbb{Z}\left[\frac{1}{p}\right]$ (why?).
  PRAC Verify that $\mathbb{Z}\left[\frac{1}{p}\right]$ is indeed a subgroup.
  (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 $H \cap Z(G)$.

Extra credit

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

*7. For G let $G^p = \langle\{g^p \mid g \in G\}\rangle$ be the subgruop generated by the pth powers.
  (a) Show $G^p \lhd G$ and that every element of G/G^p has order dividing p.
  (b) Suppose G is a finite commutative p-group. Show that $X \subset G$ generates G iff its image in G/G^p generates that group. In particular, a minimal generating set has cardinality $\dim_{\mathbb{F}_p} G/G^p = \log_p [G : G^p]$.

RMK We will see later that in any finite p-group, X generates G iff its image generates $G/G'G^p$ where G' is the derived (commutator) subgroup.

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

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?