Math 516 **Fall 2008** **Radford**

Written Homework # 1

Due at the beginning of class 09/12/08

---

1. Let G be a group and $a \in G$. Recall a^n is defined by $a^n = \begin{cases} e & : \ n = 0; \\ a^{n-1}a & : \ n > 0; \\ (a^{-1})^{-n} & : \ n < 0 \end{cases}$

(a) Let $m \geq 0$. Show, by induction, that $a^{m+n} = a^m a^n$ for all $n \geq 0$.

(b) Use part (a) to show that $a^{m+n} = a^m a^n$ for all $m, n \in \mathbf{Z}$.

(c) Use part (b) to show that $a^{mn} = (a^m)^n$ for all $m, n \in \mathbf{Z}$.

2. Suppose that $n \geq 3$. We have shown that the dihedral group D_{2n} has order $2n$ and has elements (reflections) r, s which can be thought of as the permutations of $\mathbf{Z}_n$ defined by

$$r(i) = i + 1 \qquad \text{and} \qquad s(i) = -i$$

for all $i \in \mathbf{Z}_n$. We think of $\mathbf{Z}_n$ as the group under addition modulo n.

(a) Show that $s^2 = I = r^n$, $srs = r^{n-1} = r^{-1}$. (In particular $s^{-1} = s$.)

(b) Show that $D_{2n} = \{\mathrm{I}, r, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\}$.

(c) Use part (a) to show that $sr^\ell s = r^{(n-1)\ell} = r^{-\ell}$ for all $0 \leq \ell$.

(d) Use part (c) to find a formula of the form $(r^\ell s^i)(r^{\ell'} s^{i'}) = r^{\ell''} s^{i''}$, where $0 \leq i, i' \leq 1$ and $0 \leq \ell, \ell' \leq n - 1$. (Find integers i'' and ℓ''.)

Suppose that $f : X \longrightarrow X'$ is a function. For $A \subseteq X$ set $f(A) = \{f(x) \,|\, x \in A\}$ and for $A' \subseteq X'$ set $f^{-1}(A') = \{x \in X \,|\, f(x) \in A'\}$.

3. Suppose $f : G \longrightarrow G'$ is a group homomorphism and $a \in G$.

(a) Suppose that $A \leq G$. Show that $f(A) \leq G'$. (Thus $\mathrm{Im}\, f = f(G) \leq G'$.)

(b) Suppose that $A' \leq G'$. Show that $f^{-1}(A') \leq G$. (Thus $\mathrm{Ker}\, f = f^{-1}(\{e\}) \leq G$.)

(c) Let $a \in G$. Show that $f(a^n) = f(a)^n$ for all $n \in \mathbf{Z}$. You may assume that $f(e) = e'$ and $f(a^{-1}) = f(a)^{-1}$.

(d) Show that $|f(a)|$ infinite implies $|a|$ infinite. (This is equivalent to $|a|$ finite implies $|f(a)|$ finite.)

(e) Suppose that $|a|$ is finite. Show that $|f(a)|$ is finite and divides $|a|$.

(f) Suppose that f is an isomorphism and $|a|$ is finite. Show that $|f(a)|$ is finite and $|a| = |f(a)|$.

(g) Let $n \geq 1$. Determine when $\mathbf{Z}_{n^2} \simeq \mathbf{Z}_n \times \mathbf{Z}_n$.

4. Let $G = H(\mathbf{R})$ be the Hiesenberg group, where $\mathbf{R}$ is the field of real numbers, and consider the subset $A = \{ \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix} \mid a \in \mathbf{R}\}$ of G.

(a) Determine whether or not A is a subgroup of G.

(b) Find $\mathrm{C}_G(A)$.

(c) Find $\mathrm{N}_G(A)$.

(d) Determine whether or not $A = \{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix} \mid a, b \in \mathbf{R}\}$ is a subgroup of G.

5. Let $G = <a>$ be a cyclic group of order 33.

(a) Find the number of subgroups of G.

(b) Find $|a^{-91}|$.

(c) List the elements of G in the form a^ℓ, where $0 \leq \ell < 33$, which are *not* generators.

(d) List the elements of $<a^{12}>$ in the form a^ℓ, where $0 \leq \ell < 33$.