Abstract Algebra Prelim Aug. 2011

1. (a) Prove the division algorithm in $\mathbf{Z}$: if a and b are in $\mathbf{Z}$ and $b \neq 0$ then there are q and r in $\mathbf{Z}$ such that (i) $a = bq + r$ and (ii) $0 \leq r < |b|$. (In fact q and r are unique, but you don't need to show that.)

   (b) Use part a to show every nonzero subgroup of $\mathbf{Z}$ has the form $n\mathbf{Z}$ for a unique $n \geq 1$.

2. The commutator subgroup of a group G, denoted by G', is the subgroup generated by all commutators $[x, y] = xyx^{-1}y^{-1}$ for all $x, y \in G$.

   Let $p > 2$ be an odd prime and define

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, c \in (\mathbf{Z}/p\mathbf{Z})^\times,\ b \in \mathbf{Z}/p\mathbf{Z} \right\} \subset \mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z}).$$

   (a) Show that $\left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbf{Z}/p\mathbf{Z} \right\}$ is a cyclic group of order p.

   (b) Show that G' is the group in part a.

   (c) Show that $G/G' \cong (\mathbf{Z}/p\mathbf{Z})^\times \times (\mathbf{Z}/p\mathbf{Z})^\times$.

3. (a) For a commutative ring R and R-module M, define what it means to say M is a cyclic R-module.

   (b) For any matrix $A \in \mathrm{M}_n(\mathbf{R})$, we can make $\mathbf{R}^n$ into an $\mathbf{R}[t]$-module by declaring that for any polynomial $f(t) = c_0 + c_1 t + \cdots + c_d t^d$ in $\mathbf{R}[t]$ and vector v in $\mathbf{R}^n$, $f(t)v = f(A)v = (c_0 I + c_1 A + \cdots + c_d A^d)v$.

   Determine, with explanation, whether $\mathbf{R}^n$ is a cyclic $\mathbf{R}[t]$-module for each of the following choices of A:

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ on } \mathbf{R}^2, \qquad A = \begin{pmatrix} 2 & 3 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} \text{ on } \mathbf{R}^3.$$

4. Show that a finite group whose only automorphism is the identity mapping must be trivial or have order 2.

5. Let d be a nonsquare integer and α be nonzero in $\mathbf{Z}[\sqrt{d}]$ with norm N, so $N = \alpha\overline{\alpha}$. Show the principal ideal (α) in $\mathbf{Z}[\sqrt{d}]$ has index $|N|$. That is, show $\mathbf{Z}[\sqrt{d}]/(\alpha)$ has order $|N|$. (Hint: Consider the chain of ideals $\mathbf{Z}[\sqrt{d}] \supset (\alpha) \supset (N)$.)

6. Give examples as requested, with brief justification.

   (a) An infinite abelian group in which every element has finite order.

   (b) An infinite field of characteristic p.

   (c) An integral domain which does not have unique factorization.

   (d) An irreducible polynomial in $\mathbf{Z}[t]$ of degree 8.