Instructions: *Do all three problems in part **A**, two of the three problems in part **B**, and one of the three problems in part **C** for a total of **6** problems.* Answer each problem on a separate sheet, and be sure to write the number for each problem you work out, and your name clearly at the top of each page you turn in for grading. You have three hours. Good luck!

A. Do *all* of the following.

A.1. Let G be a group and let Z denote the center of G.

(a) Show that Z is a normal subgroup of G.

(b) Show that if G/Z is cyclic, then G must be abelian.

A.2. Suppose that R is a non-zero commutative ring and let x be an indeterminate.

(a) Prove: If R is a field, then the polynomial ring $R[x]$ is a PID (principal ideal domain).

(b) Show that if R is *not* a field, then $R[x]$ is *not* a PID.

A.3. Let R be a ring.

(a) What does it mean for an R-module M to be a *free* R-module? (You do not need to explain what an R-module is.)

(b) Give an example of a $\mathbb{Z}$-module that is not free. Give an example of a $\mathbb{Q}[x]$-module that is not free.

(c) Let $A = \mathbb{Z}\left[\frac{1}{2}\right]$ be the subring of $\mathbb{Q}$ generated by $\mathbb{Z}$ and $\frac{1}{2}$. Regard A as a $\mathbb{Z}$-module. Is A finitely-generated as a $\mathbb{Z}$-module? Is A free as a $\mathbb{Z}$-module?

B. Do *two* of the following.

B.1. Let p be a prime number.

(a) Prove that every group of order p^2 is abelian.

(b) Exhibit a non-abelian group of order p^3.

(c) How many non-isomorphic abelian groups of order p^5 are there? List them.

B.2. Let R be a commutative ring with identity and let I and J be ideals of R.

(a) Define

$$(I : J) := \{r \in R : rx \in I \text{ for all } x \in J\}.$$

Show that $(I : J)$ is an ideal of R containing I.

(b) Show that if P is a prime ideal of R and $x \notin P$, then $\big(P : \langle x\rangle\big) = P$, where $\langle x\rangle$ denotes the principal ideal generated by x.

B.3. Let R be a ring and let $f : M \to N$ be a *surjective* homomorphism of R-modules, where N is a free R-module. Show that there exists an R-module homomorphism $g : N \to M$ such that $f \circ g = 1_N$. Show that $M = \mathrm{Ker}(f) \oplus \mathrm{Im}(g)$.

C. Do *one* of the following.

C.1. Let G be a finite group with n elements and consider G acting on the set of subsets $X \subseteq G$ by left translation: $gX := \{\, gx \mid x \in X \,\}$. If $A \subset G$ is a *subgroup* with k elements, then as you know, $k|n$ and the orbit of A has n/k elements. In this problem, you will prove a converse. Assume only that A is a subset with cardinality k (do not assume $k|n$ until part (d)).

(a) Show that A has a translate bA containing 1_G.

(b) The stabilizer of $X \subseteq G$, denoted $\operatorname{stab} X$, is $\{\, g \in G \mid gX = X \,\}$. State a theorem that relates the cardinality of the stabilizer of X to the cardinality of the orbit of X.

(c) Show that the stabilizer of bA (from part (a)) is contained in bA. Show that for any $y \in G$, $\operatorname{stab}(yX) = y\,(\operatorname{stab} X)\,y^{-1}$; deduce that the cardinality of the orbit of A is $\geq n/k$.

(d) Show that if the orbit of A has exactly n/k elements, then bA (from part (a)) is a subgroup of G.

C.2. Let F be a field and let x be an indeterminate. Let G be a finite subgroup of the multiplicative group of F.

(a) Explain why any $a_0 + \cdots + a_n x^n \in F[x]$ can have no more than n distinct roots in F.

(b) Let e be the smallest positive integer such that $g^e = 1$ for all $g \in G$. Using part a, show that $|G| \leq e$.

(c) Show that $|G| = e$.

(d) Explain why $|G| = e$ implies that G is cyclic. (You may use the structure theorem for finitely-generated abelian groups.)

C.3. Let F be a field and let x be an indeterminate. Let M be a cyclic $F[x]$-module that is *not* free. Suppose the ideal $\{\, g \in F[x] \mid gm = 0 \;\forall m \in M \,\}$ is generated by

$$f(x) = a_0 + \cdots + a_n x^n \in F[x].$$

(a) Show that M is finite-dimensional *as an F-module*.

(b) Show that $m \mapsto xm$ is an F-linear map of M to M.

(c) Exhibit a basis for M as an F-module.

(d) Describe the action of x on M in terms of the basis you exhibited.