1 Groups

*Do any two problems from this section.*

1. Classify up to isomorphism all groups of order 175.

2. Let $H$ and $N$ be subgroups of a group $G$ with $N$ normal. Prove that $NH = HN$ and that this set is a subgroup of $G$.

3. Do two parts to receive full credit.
   
   (a) Let $G$ be the multiplicative group of all nonsingular $2 \times 2$ matrices with rational numbers. Show that $g = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ has order 4 and $h = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ has order 3, but that $gh$ has infinite order.
   
   (b) Show that the additive group $H = (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}$ contains nonzero elements $a, b$ of infinite order such that $a + b$ is nonzero and has finite order.

4. Prove that every finitely generated subgroup of the additive group of rational numbers is cyclic.

2 Rings

*Do two problems from this section. One problem should include either Problem 1 or 2 (but not both).*

1. The following is a well known fact: if $K$ is a commutative ring with identity and $I$ is an ideal of $K$, then $K/I$ is a field if and only if $I$ is a maximal ideal of $K$. Answer all the parts to receive full credit.

   (a) Find all the maximal ideals of $\mathbb{Z}$. (You may use the fact that every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$.)

   (b) Determine whether the ideal $(3, x)$ is a maximal ideal in $\mathbb{Z}[x]$.

   (c) Determine whether the ideal $(x)$ is a maximal ideal in $\mathbb{Z}[x]$. 
2. Do all the parts to receive full credit.
   (a) Define prime ideal and maximal ideal in a commutative ring $R$ with identity.
   (b) Let $R$ and $S$ be commutative rings with identities $1_R$ and $1_S$, respectively, and let $f : R \to S$ be a ring homomorphism such that $f(1_R) = 1_S$. If $P$ is a prime ideal of $S$ show that $f^{-1}(P)$ is a prime ideal of $R$.
   (c) Let $f$ be as in part (b). If $M$ is a maximal ideal of $S$, is $f^{-1}(M)$ a maximal ideal of $R$? Prove that it is or give a counter example.

3. Let
   \[ A = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a + c = b + d, \ a, b, c, d \in \mathbb{Z} \right\}. \]
   It is easy to see that $A$ is a subring of $M_2(\mathbb{Z})$ (the ring of $2 \times 2$ matrices with elements from $\mathbb{Z}$). Do the two parts to receive full credit.
   (a) Let $R$ be the ring of $2 \times 2$ lower triangular matrices $\begin{bmatrix} m & 0 \\ n & p \end{bmatrix}$ with elements from $\mathbb{Z}$. Consider the map $f : R \to A$ defined by
      \[ f \left( \begin{bmatrix} m & 0 \\ n & p \end{bmatrix} \right) = \begin{bmatrix} m - n & m - n - p \\ n & n + p \end{bmatrix}. \]
      Is $f$ a homomorphism of rings? Justify the answer.
   (b) Are the rings $R$ and $A$ isomorphic? Explain.

4. Show that a proper ideal $M$ in a commutative ring $R$ is maximal if and only if for every $r \in R \setminus M$ there exists $x \in R$ such that $1 - rx \in M$.

3 Fields
Do any two problems from this section.

1. Prove that $\mathbb{Q}(\sqrt{3} + \sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Describe the lattice of subgroups of $\text{Gal}(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q})$ and the lattice of subfields of $\mathbb{Q}(\sqrt{3}, \sqrt{5})$.

2. Do all the parts to receive full credit.
   (i) Show that $g = X^3 - 3X - 1$ is an irreducible polynomial over $\mathbb{Q}$.
   (ii) It is known that there is a simple extension field $\mathbb{Q}(u)$ of $\mathbb{Q}$ such that $u$ is a root of $g$ and $[\mathbb{Q}(u) : \mathbb{Q}] = 3$. How is $\mathbb{Q}(u)$ defined? List the elements of a basis of $\mathbb{Q}(u)$ over $\mathbb{Q}$.
   (iii) Show that there exists a splitting extension $K$ of $g$ with $[K : \mathbb{Q}] \leq 6$.

3. Prove that one of 2, 3 or 6 is a square in the finite field $\mathbb{F}_p$ for every prime $p$. Conclude that the polynomial
   \[ x^6 - 11x^4 + 36x^2 - 36 = (x^2 - 2)(x^2 - 3)(x^2 - 6) \]
   has a root modulo $p$ for every prime $p$ but has no root in $\mathbb{Z}$. 