Math 113, Section 1, Fall 2006 (Caviglia) **FINAL**

Open book, open notes. In your proofs you may use any results from the lectures, from the parts of the textbook we covered, or from the homework exercises. Explain your answer.

(1) [**10 Points**] Let G be a finite Abelian group. Let H be a subgroup of G and let n be a fixed positive integer. Define $L = \{g \in G | g^n \in H\}$.
  (a) Prove that $|L|$ divides $|G|$.
  (b) Prove that if the number of elements in $\{g \in G | g^n \notin H\}$ is a divisor of $|G|$ then $|L| = |G|/2$.

(2) [**10 Points**] Let H and K be two groups.
  (a) Prove that $(H \times K)/(H \times \{e_K\})$ is isomorphic to K.
  (b) If $G = \langle g \rangle$ and H is a non-trivial subgroup of G, show that G/H is a finite group.
  (c) For $n, m > 1$ show that the following group is not cyclic: $(n\,\mathbb{Z}) \times (m\,\mathbb{Z})$.

(3) [**10 Points**] Prove or find a counterexample to the following statement:
Let G be a group, and let n be a fixed positive integer.
Then $\{g \in G | ord(g)$ divides $n\}$ is a subgroup of G.

(4) [**10 Points**] How many distinct group homomorphisms there are from $\mathbb{Z}$ into $\mathbb{Z}_{20}$? (explain) How many of them are injective? How many of them are surjective?

(5) [**10 Points**] Let $\phi : \mathbb{Q}[X] \to \mathbb{R}$ be the evaluation homomorphism at $\sqrt{5} + 1$.
  (a) Describe the image of such homomorphism.
  (b) Compute $Ker(\phi)$.
  (c) Is the image of ϕ a field? Explain.

(6) [**10 Points**] (a) *True or False?*: The ring $\mathbb{Z}$ has only a finite number of maximal ideals.
(b) Let R be a commutative ring with precisely only one maximal ideal, call it M. Prove that the set of invertible elements of R is exactly $R \setminus M$

(7) [**10 Points**] Let G be a group (not necessarily finite) and let H be a normal subgroup of G. Assume that H is finite and that $|H|$ is odd. Prove that if aH is an element of order 2 in G/H then there exists an element $a_1 \in G$ of order 2 with $aH = a_1 H$.

(8) [**10 Points**] Let R be a commutative ring. Given an ideal I of R and an element $f \in R$, define the set $I : f$ as $\{r \in R | rf \in I\}$.
  (a) Prove that $I : f$ is an ideal of R.
  (b) If $R = \mathbb{Z}$, what is $\langle 6 \rangle : 2$?
  (c) Is it true, in general, that $\{i \cdot f | i \in (I : f)\} = I$? Prove it or find a counterexample.

(9) [**10 Points**] Compute the remainder of $p(X)$ divided by $f(X)$ for the following pairs of polynomials:
  (a) $p(X) = X^{100} + X^2 + [2]X + [3]$, $f(X) = X - [3]$ in $\mathbb{Z}_5[X]$.
  (b) $p(X) = [2]X^5 + [3]X^2 + [1]$, $f(X) = [3]X^2 + X + [2]$ in $\mathbb{Z}_7[X]$.

(10) [**10 Points**]
  (a) Find two binary operations † and $*$ on $\mathbb{Z}$ which give $\mathbb{Z}$ a ring structure such that 2 and 3 are the identities with respect to † and $*$.
  (b) Let G be a ring and let $\phi : G \to S$ be a bijection into a set S. Define a ring structure on S (i.e. find two binary operations in order to make S into a ring) for which ϕ becomes an isomorphism of rings. Do you have to verify that S is a ring with respect these two newly defined binary operations? (explain)