Homework 2, Math 401

due on January 22, 2020

Before you start, please read the syllabus carefully.

Given a ring $(R, +, \cdot)$, we always use 0_R and 1_R to denote the identity w.r.t $+$ and $\cdot$. When there is no confusion, we will simply write 0 and 1.

Recall the definition of homomorphisms. A map $f : A \to B$ between two groups is called a *group homomorphism* if $f(a_1 + a_2) = f(a_1) + f(a_2)$. A map $f : A \to B$ between two rings is called a *ring homomorphism* if: $f(a_1 + a_2) = f(a_1) + f(a_2)$ and $f(a_1 \cdot a_2) = f(a_1) \cdot f(a_2)$ and $f(1) = 1$.

1. Read section 1.1 on *proof by induction* in case you haven't seen this before.

2. Given a ring $(R, +, \cdot)$ with 1_R and 0_R to be the identity w.r.t $\cdot$ and $+$. Define

$$(-1)_R := -1_R,$$

   and inductively for $k > 1$ that

$$k_R := (k-1)_R + 1_R, \qquad (-k)_R := (-k+1)_R + (-1)_R.$$

   Define the map $f : \mathbb{Z} \to R$ from the ring of integers to R to be $f(n) = n_R \in R$. Prove that f is a ring homomorphism. (Hint: use induction somewhere).

3. Prove that $(\mathbb{Q}\backslash\{1\}, \oplus)$ is a group where

$$a \oplus b := a + b - a \times b.$$

4. Denote the group $A = (\mathbb{Q}\backslash\{1\}, \oplus)$ and $B = (\mathbb{Q}\backslash\{0\}, \times)$. Define $f : A \to B$ that $f(a) = 1 - a$. Prove that f is a group homomorphism.

5. Denote the group $A = (\mathbb{R}, +)$ and $B = (\mathbb{R}\backslash\{0\}, \times)$. Prove that the usual exponential map $\exp : A \to B$ is a group homomorphism.
   Bonus: Can you define a group homomorphism $g : B \to A$ such that $g \circ f : A \to A$ is identity? If yes, write down the definition of g. If no, explain why.

6. (a) Find all group homomorphisms from $(\mathbb{Z}, +)$ to itself.
   (b) Find all ring homomorphisms from $(\mathbb{Z}, +, \times)$ to itself.

7. Find all elements of $\mathbb{Z}_m$ that can be written as a^2 for some $a \in \mathbb{Z}_m$ for:
   (a) $m = 5$
   (b) $m = 6$
   (c) $m = 9$

8. Find all units of $\mathbb{Z}_m$ for:
   (a) $m = 5$
   (b) $m = 6$
   (c) $m = 9$
9. Find all zero-divisors of $\mathbb{Z}_m$ for:
   (a) $m = 5$
   (b) $m = 6$
   (c) $m = 9$
10. Say an integer n is written in the decimal expression $n = \sum_{0 \le i \le n} a_i 10^i$. Prove that $3|n \iff 3|\sum_i a_i$.
11. **For fun (not required as a homework):** Given an integer n. For every prime number p, there exists an integer r_p such that $n \equiv r_p^2 (\mod p)$. Does that imply that $n = r^2$ for some integer r? If yes, give a proof. If no, give a counter example.