Homework 9: Due Friday, October 9

Definition: Given a ring R, an element $e \in R$ is called an *idempotent* if $e^2 = e$. Notice that 0 and 1 are idempotents in every ring R. For a more interesting example, the element $\overline{6} \in \mathbb{Z}/10\mathbb{Z}$ is idempotent because $\overline{6}^2 = \overline{36} = \overline{6}$.

Exercises

Exercise 1: Suppose that R and S are rings and that $\varphi\colon R \to S$ is a function such that

- $\varphi(r+s) = \varphi(r) + \varphi(s)$ for all $r, s \in R$.
- $\varphi(rs) = \varphi(r) \cdot \varphi(s)$ for all $r, s \in R$.

Thus, in contrast to the definition of a ring homomorphism, we are *not* assuming that $\varphi(1_R) = 1_S$.
a. Show that $\varphi(1_R)$ is an idempotent of S.
b. Show that if φ is surjective, then $\varphi(1_R) = 1_S$.
c. Suppose that S is an integral domain and that φ is not the zero function (i.e. there exists $r \in R$ with $\varphi(r) \neq 0_S$). Show that $\varphi(1_R) = 1_S$.

Exercise 2: Consider the ring $R = \mathbb{Z} \times \mathbb{Z}$ as a direct product (so addition and multiplication are componentwise). Determine, with explanation, which of the following subsets are ideals of R:
a. $\{(a, 0) : a \in \mathbb{Z}\}$.
b. $\{(a, a) : a \in \mathbb{Z}\}$.
c. $\{(2a, 3b) : a, b \in \mathbb{Z}\}$.

Exercise 3: Find a nonconstant polynomial in $\mathbb{Z}/4\mathbb{Z}[x]$ which is a unit. Moreover, show that for every $n \in \mathbb{N}^+$, there exists a polynomial in $\mathbb{Z}/4\mathbb{Z}[x]$ of degree n which is a unit.

Problems

Problem 1: Let X be a nonempty set. Let $R = \mathcal{P}(X)$ be the power set of X, i.e. the set of all subsets of X. We define $+$ and $\cdot$ on elements of R as follows. Given $A, B \in \mathcal{P}(X)$, define

$$A + B = A \cup B \qquad \text{and} \qquad A \cdot B = A \cap B.$$

a. Show that with these operations, R is *not* a ring in general (give a specific counterexample).

Let's scrap the above operations and try again. Given two sets A and B, the symmetric difference of A and B, denoted $A \triangle B$, is

$$A \triangle B = (A \backslash B) \cup (B \backslash A)$$

i.e. $A \triangle B$ is the set of elements in exactly one of A and B. Now define $+$ and $\cdot$ on elements of R as follows. Given $A, B \in \mathcal{P}(X)$, let

$$A + B = A \triangle B \qquad \text{and} \qquad A \cdot B = A \cap B.$$

It turns out that with these operations, R is a commutative ring, although some of the axioms are a pain to check (especially associatively of $+$ and distributivity).

b. Explain what the additive identity and multiplicative identity are in this ring, and explain what the additive inverse of an element is.

Problem 2: Let R be a ring.
a. Show that if $e \in R$ is both a unit and an idempotent, then $e = 1$.
b. Show that if R is an integral domain, then 0 and 1 are the only idempotents of R.
c. Find all idempotents in $\mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/18\mathbb{Z}$.

Problem 3: For each of the following fields F, and given $f(x), g(x) \in F[x]$, calculate the unique $q(x), r(x) \in F[x]$ with $f(x) = q(x)g(x) + r(x)$ and either $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$.
a. $F = \mathbb{Z}/2\mathbb{Z}$: $f(x) = x^5 + x^3 + x^2 + \overline{1}$ and $g(x) = x^2 + x$.
b. $F = \mathbb{Z}/5\mathbb{Z}$: $f(x) = x^3 + \overline{3}x^2 + \overline{2}$ and $g(x) = \overline{4}x^2 + \overline{1}$.

Problem 4: Consider $\mathbb{R}$ and $\mathbb{C}$ as rings. Show that $\mathbb{R} \not\cong \mathbb{C}$.

Problem 5: Define $\varphi \colon \mathbb{C} \to M_2(\mathbb{R})$ by letting

$$\varphi(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Show that φ is an injective ring homomorphism (so $\mathbb{C}$ is isomorphic to the subring range(φ) of $M_2(\mathbb{R})$).

Problem 6: Let R be a ring and let I and J be ideals of R. Define the following set:

$$I + J = \{c + d : c \in I, d \in J\}.$$

a. Prove that $I + J$ is an ideal of R (it is the smallest ideal of R containing both I and J).
b. In the ring $\mathbb{Z}$, let $I = 12\mathbb{Z} = \{12k : k \in \mathbb{Z}\}$ and let $J = 21\mathbb{Z} = \{21k : k \in \mathbb{Z}\}$. Find, with proof, an $m \in \mathbb{N}$ such that $I + J = m\mathbb{Z}$.