Homework #3

Problems to hand in on Thursday, February 7, in the beginning of class. Write your answers out carefully, staple pages, and write your name and section number on each page.

1) Prove that there is no ring homomorphism[1] $\mathbb{Z}_n \longrightarrow \mathbb{Z}$ for any integer $n > 1$.

Solution. Suppose that there is a ring homomorphism $f : \mathbb{Z}_n \longrightarrow \mathbb{Z}$. Then $f(1) = 1$, and

$$0 = f(0) = f(n) = nf(1) = n,$$

which is impossible.

2) Let R be a ring and S and T subrings of R.

(a) Prove or disprove: $S \cap T$ is a subring of R.

(b) Prove or disprove: $S \cup T$ is a subring of R.

Solution.

(a) True. $S \cap T$ contains 0_R and 1_R because both S and T do. Moreover, $S \cap T$ is closed for sums and products: if $a, b \in S \cap T$, then in particular $a, b \in S$ and $a, b \in T$, so $a + b, ab, -a \in S \cap T$ because S and T are closed for sums, products, and additive inverses. We have shown that these checks are enough to prove that $S \cap T$ is a subring, in the Adventure Sheet on Rings Basics.

(b) False. In general, the union of subrings does not have to be closed for addition or multiplication. Here are some examples:

Example 1: in the ring $R = \mathbb{R}[x, y]$ of real polynomials in 2 variables, consider the subrings $S = \mathbb{R}[x]$ and $T = \mathbb{R}[y]$. Then $x \in S \cup T$, $y \in S \cup T$, but $x + y \notin S \cup T$.

Example 2: take $R = M_2(\mathbb{R})$, the ring of 2×2 matrices with real entries. The subset $S = M_2(\mathbb{Z})$ of 2×2 matrices with entries in $\mathbb{Z}$ is a subring. The subset of T of diagonal 2×2 matrices with real entries is also a subring. However, the matrices

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \in S \text{ and } B = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \in T$$

are both in $S \cup T$, but

$$A + B = \begin{pmatrix} \frac{3}{2} & 1 \\ 1 & \frac{3}{2} \end{pmatrix}$$

is not in $S \cup T$. So $S \cup T$ is not closed for addition, and cannot be a subring of R.

3) An element $r \neq 0$ in a commutative ring R is said to be a *zerodivisor* if there exists a nonzero element $s \in R$ such that $rs = 0$.

[1] REMINDER: For us, a ring homomorphism must preserve multiplicative identities.

(a) Given a nonzero element $r \in R$, prove that r is not a zerodivisor if and only if the map $R \longrightarrow R$ given by multiplication by r, meaning the map $s \mapsto rs$, is injective.

(b) Describe all the zerodivisors in $\mathbb{Z}_n$ in terms of the prime factorization of n or their greatest common divisor with n.

Solution.

(a) Suppose that r is not a zerodivisor, and consider $a, b \in R$ such that $ra = rb$. Then $r(a-b) = 0$, and since r is not a zerodivisor, we must have $a - b = 0$. This shows that multiplication by r is injective. On the other hand, if multiplication by r is an injective map, then $ra = 0$ implies that $a = 0$, and r is not a zerodivisor.

(b) If $m \in \mathbb{Z}$ is such that $[m]$ is a zerodivisor in $\mathbb{Z}_n$, that means $n \nmid m$ and there exists some $k \in \mathbb{Z}$ such that $n \nmid k$ but $n \mid km$. Equivalently, $1 < (n, m) < n$.

We will show in problem 4(e) that if $(n, m) = 1$, then m is a unit, and in problem 4(a) that units are not zerodivisors. If $1 < d = (n, m) < m$, then $n = dk$ for some $1 < k < n$, so $k \not\equiv 0 \mod n$, and $mk \equiv 0 \mod n$.

4) A *unit* u in a ring R is an invertible element, meaning there exists $s \in R$ such that $su = us = 1$.

(a) Show that if u is a unit in R, then u is not a zerodivisor.

(b) If $u \neq 0$ is not a zerodivisor in a commutative ring R, does that imply it is a unit?

(c) Show that if a and b are units, then ab is a unit.

(d) Prove or disprove: the set of all units in a commutative ring R forms a subring.

(e) Describe all the units in $\mathbb{Z}_n$ in terms of the prime factorization of n or their greatest common divisor with n.

Solution.

(a) Suppose that $ua = 0$. Then $a = u^{-1}(ua) = 0$.

(b) No! For example, in the ring $\mathbb{Z}$, the element 2 is neither a zerodivisor nor a unit.

(c) The element $b^{-1}a^{-1}$ is an inverse of ab:

$$\left(b^{-1}a^{-1}\right)(ab) = b^{-1}\left(a^{-1}a\right)b = b^{-1}b = 1$$

and

$$(ab)\left(b^{-1}a^{-1}\right) = a\left(bb^{-1}\right)a^{-1} = aa^{-1} = 1.$$

(d) False, since 0 is not a unit.

(e) The class modulo n of the integer a is invertible in $\mathbb{Z}_n$ if and only if $(a, n) = 1$. We proved in the Adventure Sheet on Arithmetic in $\mathbb{Z}_n$ that $[a]$ has an inverse whenever $(a, n) = 1$, and we proved on Quiz 3 that if $ax \cong b \mod n$ has a solution, then $(a, n) | b$. As a consequence, when we taken $b = 1$, this says that if $[a]$ has an inverse modulo n, then $(a, n) = 1$.