Problem Set 7

Problems with (HW) are due Friday 11/1 in class. Your homework should be easily legible, but need not be typed in Latex. Use full sentences to explain your solutions, but try to be concise as well. Think of your audience as other students in the class.

Problems 7.1. Prove the following basic results about rings. (Discuss one of (1)-(4), do (7)).

(1) The inverse of a unit is unique.
(2) The inverse of a unit is also a unit.
(3) A unit cannot be a zero divisor.
(4) A nonzero nilpotent element is a zero-divisor.
(5) Find the nilpotent elements of $\mathbb{Z}/8$, of $\mathbb{Z}/12$, and of $\mathbb{Z}/30$.
(6) Under what conditions on n does $\mathbb{Z}/n$ have nilpotent elements? Identify the nilpotent elements of $\mathbb{Z}/n$ using the unique factorization of n.
(7) Let F be a field and $m(x) \in F[x]$. Under what conditions on $m(x)$ does $F[x]/m(x)$ have nilpotent elements? Identify the nilpotents $a(x) \in F[x]/m(x)$ using unique factorization into irreducibles of $m(x)$ and $a(x)$.
(8) (HW) Let R and S be rings and consider $R \times S$. Identify all the units $R \times S$ by reference to the units in R and S. [You might want to consider $\mathbb{Z}/m \times \mathbb{Z}/n$ to get started.]
(9) (HW) Let R and S be rings and consider $R \times S$. Identify all the zero-divisors in $R \times S$ by reference to the zero-divisors in R and S. [You might want to consider $\mathbb{Z}/m \times \mathbb{Z}/n$ to get started.]

Problems 7.2.

(1) Let R be an integral domain. Show that the cancellation law holds: If $ar = as$ then $r = s$.
(2) (HW) Let R be an integral domain that is finite. Show that R is a field. (For a nonzero $a \in R$, consider the function $R \longrightarrow R$ that takes r to $a * r$.)

Problems 7.3. (Discussion) Suppose R, S are subrings of a ring T.

(1) Show that $R \cap S$ is also a subring of T.
(2) Give an example to show that $R \cup S$ may not be a ring.

Problems 7.4. (Discussion) Let $\varphi : R \longrightarrow S$ be a ring homomorphism.

(1) Show that for any subring R' in R, the image $\varphi(R')$ is a subring of S.

(2) Show that any subring S' of S, the preimage $\varphi^{-1}(S')$ is a subring of R.

Problems 7.5.

(1) (HW) Give an example of two polynomials of degree 2 in $\mathbb{Z}/8[x]$ such that their product has degree 1. Is this possible in $\mathbb{Z}/4[x]$ and $\mathbb{Z}/6[x]$?

(2) (HW) Give an example to show that the analogue of Lemma 1.3.1 does not hold in the polynomial ring over $\mathbb{Z}/4$. If you can, generalize to arbitrary $\mathbb{Z}/n$ for n not a prime.

Problems 7.6.

(1) (HW) Let F be a field (any field will do). Find the gcd of $x^5 - 1$ and $x^3 - 1$ using the Euclidean algorithm. Write the gcd as a polynomial combination of $x^5 - 1$ and $x^3 - 1$. Write the matrices used in the matrix version of the Euclidean algorithm.

(2) Show that $x^d - 1$ divides $x^n - 1$ if and only if d divides n. (Hint. substitute x^b for y in $y^a - 1 = (y-1)(y^{a-1} + y^{a-2} + \cdots + y + 1)$)

(3) (HW) More generally, if r is the remainder when n is divided by d, then $x^r - 1$ is the remainder when $x^n - 1$ is divided by $x^d - 1$.

(4) (Challenge) Let m and n be positive integers and $d = \gcd(m, n)$. Show that $\gcd(x^n - 1, x^m - 1) = x^d - 1$.