Problem Set 8

Problems with (HW) are due Thursday 10/27 at 11:00 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.

Exercises 8.1. (HW) This problem fleshes out some details in the proof of Theorem 3.3.8: A_n is simple for $n > 5$.

(a) Within the alternating group A_n for each $i = 1, \ldots, n$, let $G_i = \{\sigma \in A_n : \sigma(i) = i\}$. Show that G_i is a subgroup of A_n.

(b) Find a $\pi \in A_n$ such that each $G_i = \pi G_j \pi^{-1}$.

(c) Justify the statement in the fourth paragraph of the proof of 3.3.8 "Then $(\tau\sigma\tau^{-1})\sigma^{-1} \in N$ and straightforward computation shows $\tau\sigma\tau^{-1}\sigma^{-1}(c) = c$."

(d) Justify the statement in the fifth paragraph of the proof of 3.3.8 "$(\tau\sigma\tau^{-1})\sigma^{-1} \in N$ and $\tau\sigma\tau^{-1}\sigma^{-1}(b) = b$."

Exercises 8.2. Prove the following basic results about rings. (Discuss one (a)-(d).

(a) The inverse of a unit is unique.

(b) The inverse of a unit is also a unit.

(c) A unit cannot be a zero divisor.

(d) A nilpotent element is a zero-divisor.

(e) Find the nilpotent elements of $\mathbb{Z}/8$, of $\mathbb{Z}/12$, and of $\mathbb{Z}/30$.

(f) (HW) Under what conditions on n does $\mathbb{Z}/n$ have nilpotent elements?

(g) (HW) Identify the nilpotent elements of $\mathbb{Z}/n$ using the unique factorization of n.

(h) (HW) 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 $a(x)$.

(i) (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.]

(j) (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.]

Exercises 8.3. (HW)

(a) 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 $a * r$.)

Exercises 8.4. (Discussion) Suppose R, S are subrings of a ring T.

(a) Show that $R \cap S$ is also a subring of T.

(b) Give an example to show that $R \cup S$ may not be a ring.

Exercises 8.5. (Discussion) Let $\varphi : R \longrightarrow S$ be a ring homomorphism.

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

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

Exercises 8.6.

(a) (Discussion) 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 $\mathbb{Z}/6[x]$?

(b) (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.

Exercises 8.7.

(a) (Discussion) 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 (see p. 6 in the notes).

(b) (HW) Show that $x^d - 1$ divides $x^n - 1$ if and only if d divides n.

(c) (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 $x^d - 1$.

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