Assignment 3 – All 2 parts – Math 412

Due in class: Thursday, Sept. 19, 2019

Textbook exercises:[1]

Section 2.3: 12 (WI), 13

Section 3.2: 18 (WI), 38 (WI)

Other exercises:

(1) Find the multiplicative inverses of the following elements a of $\mathbf{Z}/n\mathbf{Z}$ (i.e. find $u \in \mathbf{Z}/n\mathbf{Z}$ such that $au = 1$).

(a) $n = 11$ and $a = 4$.

(b) $n = 11$ and $a = 8$.

(c) $n = 12$ and $a = 7$.

(2) Show by computation that $\mathbf{Z}/7\mathbf{Z} = \{0\} \cup \{[3]^i : i = 0, 1, \ldots, 5\}$, i.e. every nonzero number in $\mathbf{Z}/7\mathbf{Z}$ is a power of 3. (Remark: it can be shown that if p is a prime number, then there is a number a such that every nonzero number in $\mathbf{Z}/p\mathbf{Z}$ is a power of a; such an a is called a *primitive root modulo* p. Fixing a instead, in 1927, Emil Artin conjectured that if $a \in \mathbf{Z}$ is not a square nor -1, then a is a primitive root modulo p for infinitely many p. This conjecture is wide open: it is not known for any value of a. Various interesting partial result are known; for instance, the conjecture is true for at least one of $2, 3$, or 5.)

(3) Consider the set $\mathbf{Z}$ with the following new binary operations $\oplus$ and $\odot$:

$$a \oplus b = a + b - 1 \quad \text{and} \quad a \odot b = a + b - a \cdot b,$$

where $+$ and $\cdot$ denote the usual addition and multiplication of integers. Show that $(\mathbf{Z}, \oplus, \odot)$ is a ring! (Hint: the additive identity is 1 and the multiplicative identity is 0.)

(4) Let R be a ring. An element $a \in R$ is called a *zerodivisor* if $a \neq 0$ and there is a nonzero $b \in R$ such that $ab = 0$ or $ba = 0$ (a nonzero a that is not a zerodivisor is called a *nonzerodivisor*). An element $a \in R$ is called a *unit* if there is an element $u \in R$ such that $au = 1 = ua$ (we also say that a is *invertible* or that a has a (*multiplicative*) *inverse*).

[1] From Hungerford's *Abstract algebra, An introduction, Third edition*

(a) Show that a unit cannot be a zerodivisor.

(b) Show that if $a \in R$ is a nonzerodivisor, then it satisfies the Cancellation Law, i.e. for all $b, c \in R$, $ab = ac$ implies $b = c$ and $ba = ca$ implies $b = c$.

(c) Let $a, b \in R$. Show that if ab is a zerodivisor, then a is a zerodivisor or b is a zerodivisor.

(d) Show that if $a, b \in R$ are both units, then so is ab.

(e) Suppose R is commutative and that $a \in R$ is a zerodivisor. Let $b \in R$. Show that if $ab \neq 0$, then ab is a zerodivisor.