Problem Set 7

(Hand in all.)

(1) [Jacobson p. 97 #1] Show that the matrix
$$\begin{pmatrix} 1 & 4 & 1 \\ 0 & 1 & -1 \\ -3 & -6 & -8 \end{pmatrix}$$
is invertible in $M_3(\mathbb{Z})$ and find its inverse.

(2) [Jacobson p. 97 #2] Prove that if R is a commutative ring then $AB = \mathbb{1}$ in $M_n(R)$ implies $BA = \mathbb{1}$. (This is not always true for noncommutative R.)

(3) [Jacobson p. 97 #7] Determine $C(S)$ (the set of all elements commuting with S) where S is the single matrix $N = \mathbf{e}_{12} + \mathbf{e}_{23} + \cdots + \mathbf{e}_{n-1,n}$.

(4) Show that the set of ideals in a ring R forms a monoid under multiplication. Do they satisfy the distributive law $I(J + K) = IJ + IK$?

(5) State and prove a uniqueness result for Hermite normal form. (We know it isn't unique as a matrix, unlike rref for fields. So, what attributes are unique (i.e. constitute invariants of the original matrix)?

(6) Prove that ± 3 are not of the form $m^2 - 10n^2$ ($m, n \in \mathbb{Z}$).

(7) [Jacobson p. 103 #6] Let R be a commutative ring and N denote the set of nilpotent elements of R. Show that N is an ideal and that R/N contains no non-zero nilpotent elements.

(8) [Jacobson p. 109 #2] (a) Given $u \in R^*$ and $\eta\colon R \to R'$ a homomorphism, show that $\eta(u)$ is a unit in R'. (b) Suppose η is surjective. Does this imply that (under η) the group of units R^* surjects onto $(R')^*$?

(9) [Jacobson p. 110 #4] Show that if R is a commutative ring of prime characteristic p, then $\phi\colon R \to R$ defined by $a \mapsto a^p$ is a homomorphism (also called an "endomorphism of R"). Is this an automorphism?

(10) [Jacobson p. 110 #5] Let F be a finite field of characteristic p (a prime). Show that $p - 1 \big| |F| - 1$. Hence conclude that if $|F|$ is even then the characteristic is 2. (We shall see later that $|F|$ is a power of p.)

(11) [Jacobson p. 110#7] If S is a subset of a ring (field) R then the *subring* (*subfield*) *generated by* S is defined to be the intersection of all the subrings (subfields) containing S. If this is R itself then S is called a *generating set* for R. Show that if η_1 and η_2 are homomorphisms from R to R' which agree on the elements of a generating set $S \subset R$, then $\eta_1 = \eta_2$.

(12) Let $R = \mathbb{Z}[\alpha]$, where $\alpha := \frac{1+\sqrt{-19}}{2}$. Show that R is *not* Euclidean, in contrast to problem (8) from last week. [Hint: let s be a nonzero nonunit of minimal $\delta(s)$, and consider the image of α in $R/(s)$. Use the fact that $\alpha^2 - \alpha + 5 = 0$, and the result of last week's problem (7).]