Math 404 – Spring 2025 – Harry Tamvakis
PROBLEM SET 2 – Due February 13, 2025

Reading for this week: Review of basic linear algebra, and Sections 1.1-1.4, 2.1-2.3 of the textbook. (We will not require Theorem 2.5, only its Corollary 2.9. A different proof of Corollary 2.9 will be given in class).

Problems

1) Let F be a field containing exactly 16 elements. Prove or disprove that the characteristic of F is equal to 2.

2) Let R be a non-zero commutative ring. A *zero-divisor* is an element a such that $ax = 0$ for some non-zero x in R. Prove that if R has only finitely many elements then every element of R is either a zero-divisor or a unit. Deduce that every finite integral domain is a field.

3) (a) Define a ring homomorphism $\phi : \mathbb{R}[x] \to \mathbb{R}$ by setting $\phi(f(x)) := f(2)$, for any $f \in \mathbb{R}[x]$. Since $\mathbb{R}[x]$ is a principal ideal domain, the ideal $\operatorname{Ker}\phi$ may be generated by a single polynomial $g \in \mathbb{R}[x]$. Find (with proof) such a polynomial $g(x)$.

(b) Let $\mathbb{Q}[\sqrt{2}]$ denote the ring consisting of all real numbers of the form $a + b\sqrt{2}$, where $a, b \in \mathbb{Q}$. Define a ring homomorphism $\psi : \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{2}]$ by setting $\psi(f(x)) := f(\sqrt{2})$, for any $f \in \mathbb{Q}[x]$. Since $\mathbb{Q}[x]$ is a principal ideal domain, the ideal $\operatorname{Ker}\psi$ may be generated by a single polynomial $h \in \mathbb{Q}[x]$. Find (with proof) such a polynomial $h(x)$.

4) Show that the polynomial ring $\mathbb{Z}[x]$ is not a principal ideal domain. Do this by finding an ideal in $\mathbb{Z}[x]$ which is not principal (and prove that this is the case).

5) Let F be a field of characteristic $p > 0$. Prove that the map $\phi : F \to F$ defined by $\phi(x) := x^p$ is a ring homomorphism. This map is called the *Frobenius homomorphism*. Show also that ϕ is injective.

6) The real numbers form a ring; let σ be an automorphism of this ring (i.e. σ is a ring isomorphism $\mathbb{R} \to \mathbb{R}$).

(a) Show that if k is an integer, then $\sigma(k) = k$.

(b) Show that $\sigma(q) = q$ for any rational number q.

(c) Prove that if $x > 0$, then $\sigma(x) > 0$. Also show that if $x > y$, then $\sigma(x) > \sigma(y)$.

(d) Show that $\sigma(x) = x$, for all real numbers x.

In other words, the only automorphism of $\mathbb{R}$ is the identity. By the way, this is *false* for $\mathbb{C}$; in fact, there are infinitely many automorphisms of $\mathbb{C}$. Can you find one besides the identity?

7) Let R denote the set of sequences $a = (a_1, a_2, \ldots)$ of real numbers which are eventually constant, i.e., such that $a_n = a_{n+1} = \cdots$ for sufficiently large n. Addition and multiplication in R is defined componentwise, that is, addition is vector addition and $ab := (a_1b_1, a_2b_2, \ldots)$. Check that R is a ring (you do not have to write down the proof). Determine (with proof) all the maximal ideals of R.

8) Let R be a commutative ring. Consider the set of all infinite sequences $\{a_i\}_{i=0}^{\infty}$, with the $a_i \in R$. Add these termwise and multiply them by the rule: $\{a_i\}\{b_j\} = \{c_k\}$, where $c_k := \sum_{i=0}^{k} a_i b_{k-i}$. This makes a commutative ring. If X denotes the sequence $(0, 1, 0, 0, \ldots)$, we can identify our sequence ring with the ring of *formal power series* $\sum_{j=0}^{\infty} a_j X^j$ in the indeterminant X with coefficients in R. (These sums are not necessarily finite! *Formal* means that there is no question of convergence). Denote this ring by $R[[X]]$.

(a) Write f for a formal power series $\sum_{j=0}^{\infty} a_j X^j$ and write $f(0)$ for the constant term, a_0, of f. Prove that the map Φ defined by $\Phi(f) := f(0)$ is a surjective ring homomorphism $R[[X]] \to R$.

(b) Prove: if R is an integral domain then so is $R[[X]]$.

(c) Show that if $f(0)$ is a unit of R, then f is a unit of $R[[X]]$.

Extra Credit Problems.

EC1) This is a continuation of problem #8 above.

(a) Let K be a field. Define $K((X))$ to be the ring of formal power series in X (with coefficients in K) which involve as well a *finite* number of negative powers of X; i.e. of the form $\sum_{j \geq N}^{\infty} a_j X^j$ for some $N \in \mathbb{Z}$ (this is the ring of formal *Laurent series*.) Prove that $K((X))$ is the quotient field of $K[[X]]$.

(b) If R is a domain with quotient field K, it is not necessarily true that $K((X))$ is the quotient field of $R[[X]]$. For example, show that the quotient field of the power series ring $\mathbb{Z}[[X]]$ is *properly* contained in the field of Laurent series $\mathbb{Q}((X))$. [Hint: Consider the series for e^x.]

EC2) Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ denote the finite field with p elements, for p a prime number. Prove that the polynomial ring $\mathbb{F}_p[x]$ contains *infinitely many* irreducible polynomials.