Math 412. Comparison of Rings.

The ring $\mathbb{F}[x]$ of polynomials over an arbitrary *field* shares many properties and features with the ring $\mathbb{Z}$ of integers. Most of these special features **do not hold** (or do not even make sense!) in arbitrary rings, including polynomial rings over non-fields like $\mathbb{Z}[x]$ or $\mathbb{Z}_6[x]$, quotient rings like $\mathbb{Z}_n$ or $\mathbb{F}[x]/(f)$ or matrix rings like $M_3(\mathbb{R})$ or $M_2(\mathbb{Z})$.

IMPORTANT: The symbol $\mathbb{F}$ below stands for an arbitrary **field**. Think of $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ (where p is prime), or something more exotic like $\mathbb{Q}(i)$ or $\mathbb{R}(x)$ or even the field of four elements $\mathbb{F}_4 := \mathbb{Z}_2[x]/(x^2 + x + 1)$.

CAUTION: The definitions and theorems in the table above are paraphrased for your intuition in comparing them, and are not intended to be used as precise statements for quizzes and exams.

TABLE 1. Analogous Concepts across Different Rings.

Arbitrary Ring R	**The Ring $\mathbb{Z}$**	**The Ring $\mathbb{F}[x]$**
For $r, s \in R$, we say r **divides** s if $\exists t \in R$ such that $s = r \cdot t$.	Example in $\mathbb{Z}$: 6 divides -12 since $-12 = 6 \times (-2)$	Example in $\mathbb{Q}[x]$: $x+1$ divides (x^2-1) since $x-1 = (x+1)(x-1)$
A **zero-divisor** in R is an element r for which there exists $s \neq 0$ in R such that $rs = 0$ or $sr = 0$.	FACT: The only zero divisor in $\mathbb{Z}$ is 0.	FACT: The only zero divisor in $\mathbb{F}[x]$ is 0.
$u \in R$ is a **unit** if and only if there exists $v \in R$ such that $uv = vu = 1$. $R^\times$ denotes the set of all units in R.	Units in $\mathbb{Z}$ $= \{\pm 1\}$	Units in $\mathbb{F}[x]$ $= \{\lambda \mid \lambda \in \mathbb{F} \setminus \{0\}\}$, i.e. non-zero constant polynomials.
DEF: An element $r \in R$ is **irreducible** if its only divisors are of the form u, ur where u is a unit in R	An integer n is irreducible (A.K.A. **prime**) if and only if its only divisors are ± 1 and $\pm n$.	A polynomial $f(x)$ is **irreducible** if and only if its only divisors are of the form λ and $\lambda f(x)$ where $\lambda \in \mathbb{F} \setminus \{0\}$
No Division algorithm (no obvious way to decide when one element in R is "smaller than" another)	Given $n, d \in \mathbb{Z}$ with $d > 0$, there exist unique integers q, r such that $n = qd + r$ and $0 \leq r < d$.	Given $f, g \in \mathbb{F}[x]$ with $g \neq 0$, there exist unique polynomials q, r such that $f = qg + r$ and ($r = 0$ or) $\deg r < \deg g$.
No definition of gcd (no natural way to decide when one element in R is "larger than" another)	DEF: $\gcd(m, n)$ is the largest common divisor of n and m	DEF: $\gcd(f, g)$ is the largest degree monic common divisor of f and g
No analog of Euclidean algorithm or its corollaries	THM: $\gcd(n, m)$ is smallest positive $\mathbb{Z}$-linear combination of m and n	THM: $\gcd(f, g)$ is smallest degree monic $\mathbb{F}[x]$-linear comb of f and g
No Unique Factorization Thm (proof uses Division algorithm)	THM[1]: Every integer n can be factored as $p_1 p_2 \dots p_t$ where the p_i are prime. The p_i are unique up to re-ordering and unit multiple.	THM: Every polynomial f can be factored as $g_1 g_2 \dots g_t$ where the g_i are irreducible. The g_i are unique up to re-ordering and unit multiple.
An **ideal** of R is a non-empty subset of R closed under addition and under multiplication by element of R.	An **ideal** of $\mathbb{Z}$ is a non-empty subset of $\mathbb{Z}$ closed under addition and under multiplication by all $a \in \mathbb{Z}$.	An **ideal** of $\mathbb{F}[x]$ is a non-empty subset of $\mathbb{F}[x]$ closed under addition and under multiplication by all $g \in \mathbb{F}[x]$.
A set of **Generators** for an ideal I is any set $\mathcal{S} \subset I$ with the property that *every* element in I is an R-linear combination of the elements of $\mathcal{S}$.	THM: In $\mathbb{Z}$, all ideals are generated by one element. So an ideal of $\mathbb{Z}$ is a set of all multiples of fixed integer n.	THM: In $\mathbb{F}[x]$, all ideals are generated by one element. So an ideal of $\mathbb{F}[x]$ is a set of all multiples of a fixed polynomial $f(x)$.
Ideals may need more than one generator; in some cases, even infinitely many.	THM: Every ideal of $\mathbb{Z}$ is principal	THM: Every ideal of $\mathbb{F}[x]$ is principal
Two elements $x, y \in R$ are **congruent modulo an ideal** I if $x - y \in I$	Integers $a, b \in \mathbb{Z}$ are **congruent modulo the ideal** $n\mathbb{Z}$ if $a - b$ is a multiple of n, or equivalently, if $n \mid (a-b)$	Polynomials $g, h \in \mathbb{F}[x]$ are **congruent modulo the ideal** generated by f if $g - g$ is a multiple of f, or equivalently, if $f \mid (g-h)$
R/I is a ring whose elements are congruence classes mod I	$\mathbb{Z}_n$ is a ring whose elements are congruence classes modulo (n).	$\mathbb{F}[x]/(f)$ is a ring whose elements are congruence classes modulo (f).