is the largest power of X which occurs with nonzero coefficient; in a *monic* polynomial the coefficient of X^d is 1. We say that g *divides* f, where f, $g \in \mathbf{F}[X]$, if there exists a polynomial $h \in \mathbf{F}[X]$ such that $f = gh$. The *irreducible* polynomials $f \in \mathbf{F}[X]$ are those that are not divisible by any polynomials of lower degree except for constants; they play the role among the polynomials that the primes play among the integers. The polynomial ring has *unique factorization*, meaning that every monic polynomial can be written in one and only one way (except for the order of factors) as a product of monic irreducible polynomials. (A non-monic polynomial can be uniquely written as a constant times such a product.)

4. An element α in some extension field $\mathbf{K}$ containing $\mathbf{F}$ is said to be *algebraic* over $\mathbf{F}$ if it satisfies a polynomial with coefficients in $\mathbf{F}$. In that case there is a *unique* monic irreducible polynomial in $\mathbf{F}[X]$ of which α is a root (and any other polynomial which α satisfies must be divisible by this monic irreducible polynomial). If this monic irreducible polynomial has degree d, then any element of $\mathbf{F}(\alpha)$ (i.e., any rational expression involving powers of α and elements in $\mathbf{F}$) can actually be expressed as a linear combination of the powers $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$. Thus, those powers of α form a basis of $F(\alpha)$ over F, and so the degree of the extension obtained by adjoining α is the same as the degree of the monic irreducible polynomial of α. Any other root α' of the same irreducible polynomial is called a *conjugate* of α over $\mathbf{F}$. The fields $\mathbf{F}(\alpha)$ and $\mathbf{F}(\alpha')$ are *isomorphic* by means of the map that takes any expression in terms of α to the same expression with α replaced by α'. The word "isomorphic" means that we have a 1-to-1 correspondence that preserves addition and multiplication. In some cases the fields $\mathbf{F}(\alpha)$ and $\mathbf{F}(\alpha')$ are the same, in which case we obtain an *automorphism* of the field. For example, $\sqrt{2}$ has one conjugate, namely $-\sqrt{2}$, over $\mathbf{Q}$, and the map $a+b\sqrt{2} \mapsto a-b\sqrt{2}$ is an automorphism of the field $\mathbf{Q}(\sqrt{2})$ (which consists of all real numbers of the form $a + b\sqrt{2}$ with a and b rational). If all of the conjugates of α are in the field $\mathbf{F}(\alpha)$, then $\mathbf{F}(\alpha)$ is called a *Galois* extension of $\mathbf{F}$.

5. The *derivative* of a polynomial is defined using the nX^{n-1} rule (not as a limit, since limits don't make sense in $\mathbf{F}$ unless there is a concept of distance or a topology in $\mathbf{F}$). A polynomial f of degree d may or may not have a root $r \in \mathbf{F}$, i.e., a value which gives 0 when substituted in place of X in the polynomial. If it does, then the degree-1 polynomial $X-r$ divides f; if $(X-r)^m$ is the highest power of $X-r$ which divides f, then we say that r is a root of *multiplicity* m. Because of unique factorization, the total number of roots of f in $\mathbf{F}$, counting multiplicity, cannot exceed d. If a polynomial $f \in \mathbf{F}[X]$ has a multiple root r, then r will be a root of the *greatest common divisor* of f and its derivative f'(see Exercise 13 of § I.2).

6. Given any polynomial $f(X) \in \mathbf{F}[X]$, there is an extension field $\mathbf{K}$ of